```
--------------------------------------------------------------------------------
          %%%%%%%%%%%%%%%%%%%%%%%%%%%%-%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
          %                                                        %
          %            THE NEOPHYTE'S GUIDE TO HACKING             %
          %            ===============================             %
          %                      1993 Edition                      %
          %                 Completed on 08/28/93                  %
          %           Modification 1.1 Done on 10/10/93            %
          %           Modification 1.2 Done on 10/23/93            %
          %                           by                           %
          %%                >>>>>  Deicide  <<<<<                 %%
          %%%                                                    %%%
          %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```


```
     <   The author of this file grants permission to reproduce and   >
     <   redistribute this file in any way the reader sees fit,       >
     <   including the inclusion of this file in newsletters of any   >
     <   media, provided the file is kept whole and complete,         >
     <   without any modifications, deletions or ommissions.          >
     <   (c) 1993, Deicide                                            >
```


TABLE OF CONTENTS
==========

1. INTRODUCTION

2. ETHICS/SAFETY

3. WHERE TO START

4. PACKET-SWITCHED NETWORKS
    A. Intro to PSNs
    B. How packet-switching works
    C. The Internet
        1. Introduction
        2. Getting access
        3. FTP
    D. X.25 Networks
        1. NUAs
        2. PADs & NUIs
        3. CUGs
        4. SprintNet
        5. BT Tymnet
        6. Datapac
        7. DNIC List

5. SYSTEM PENETRATION
    A. Unix
    B. VMS
    C. MPE (HP3000 mainframes)
    D. VM/CMS
    E. Primos
    F. TOPS 10/20
    G. IRIS
    H. NOS
    I. DECServer
    J. GS/1
    K. XMUX
    L. Starmaster/PACX
    M. Access 2590
    N. PICK
    O. AOS/VS
    P. RSTS

Q. WindowsNT
R. Novell Netware
S. System75/85
T. AS400
U. TSO

6. BRUTE FORCE
A. Passwords
B. Usernames
C. Services

7. SOCIAL ENGINEERING

8. TRASHING

9. ACRONYMS

10. CONCLUSION
A. Last words
B. Recommended Reading
C. BBSes
D. References
E. And finally..
F. Disclaimer

INTRODUCTION:

Over four years ago the final version of the LOD/H's Novice's Guide to Hacking was created and distributed, and during the years since it has served as a much needed source of knowledge for the many hackers just beginning to explore the wonders of system penetration and exploration.

The guide was much needed by the throng of newbies who hadn't the slightest clue what a VAX was, but were eager to learn the arcane art of hacking. Many of today's greats and moderates alike relied the guide as a valuable reference during their tentative(or not) steps into the nets.

However, time has taken it's toll on the silicon networks and the guide is now a tad out of date. The basic manufacturer defaults are now usually secured , and more operating systems have come on the scene to take a large chunk of the OS percentile. In over four years not one good attempt at a sequel has been made, for reasons unbeknownst to me.

So, I decided to take it upon myself to create my own guide to hacking.. the "Neophyte's Guide to Hacking" (hey..no laughing!) in the hopes that it might help others in furthering their explorations of the nets.

This guide is modelled after the original, mainly due to the fact that the original *was* good. New sections have been added, and old sections expanded upon. However, this is in no means just an update, it is an entirely new guide as you'll see by the difference in size. This guide turned out to be over 4 times the size of The Mentor's guide.

Also, this guide is NOT an actual "sequel" to the original; it is not LOD/H sponsored or authorized or whatever, mainly because the LOD/H is now extinct.

One last thing.. this guide is in no way complete. There are many OS's I did not include, the main reasons being their rarity or my non-expertise with them. All the major OS's are covered, but in future releases I wish to include Wang, MVS, CICS, SimVTAM, Qinter, IMS, VOS, and many more. If you feel you could help, contact me by Internet email or on a board or net(if you can find me). Same thing applies for further expansion of current topics and operating systems, please contact me.

Ok, a rather long intro, but fuck it.. enjoy as you wish..

Deicide - deicide@west.darkside.com

ETHICS/SAFETY:

One of the most integral parts of a hacker's mindset is his set of ethics. And ethics frequently go hand in hand with safety, which is obviously the most critical part of the process of hacking and the system exploration, if you plan to spend your life outside of the gaol.

A hacker's ethics are generally somewhat different from that of an average joe. An average joe would be taught that it is bad to break laws, even though most do anyways. I am encouraging you to break laws, but in the quest for knowledge. In my mind, if hacking is done with the right intentions it is not all that criminal. The media likes to make us out to be psychotic sociopaths bent on causing armageddon with our PCs. Not likely. I could probably turn the tables on the fearmongering media by showing that the average joe who cheats on his taxes is harming the system more than a curious interloper, but I refrain.. let them wallow..

The one thing a hacker must never do is maliciously hack(also known as crash, trash, etc..) a system. Deleting and modifying files unnecessary is BAD. It serves no purpose but to send the sysadmins on a warhunt for your head , and to take away your account. Lame. Don't do it.

Anyways, if you don't understand all of these, just do your best to follow them, and take my word for it. You'll understand the reasoning behind these guidelines later.

I. Don't ever maliciously hack a system. Do not delete or modify files unnecessarily, or intentionally slow down or crash a system. The lone exception to this rule is the modification of system logs and audit trails to hide your tracks.

II. Don't give your name or real phone number to ANYONE, it doesn't matter who they are. Some of the most famous phreaks have turned narcs because they've been busted, and they will turn you in if you give them a chance. It's been said that one out of every three hackers is a fed, and while this is an exaggeration, use this as a rule and you should do fine. Meet them on a loop, alliance, bbs, chat system, whatever, just don't give out your voice number.

III. Stay away from government computers. You will find out very fast that attempting to hack a MilTac installation is next to impossible, and will get you arrested before you can say "oh shit". Big Brother has infinite resources to draw on, and has all the time it needs to hunt you down. They will spend literally years tracking you down. As tempting as it may be, don't rush into it, you'll regret it in the end.

IV. Don't use codes from your own home, ever! Period. This is the most incredibly lame thing i've seen throughout my life in the 'underground'; incredible abuse of codes, which has been the downfall of so many people. Most PBX/950/800s have ANI, and using them will eventually get you busted, without question. And calling cards are an even worse idea. Codes are a form of pseudo-phreaking which have nothing to do with the exploration of the telephone networks, which is what phreaking is about. If you are too lazy to field phreak or be inventive, then forget about phreaking.

V. Don't incriminate others, no matter how bad you hate them. Turning in people over a dispute is a terrible way to solve things; kick their ass, shut off their phones/power/water, whatever, just don't bust them. It will come back to you in the end..

VI. Watch what you post. Don't post accounts or codes over open nets as a rule. They will die within days, and you will lose your new treasure. And the posting of credit card numbers is indeed a criminal offense under a law passed in the Reagan years.

VII. Don't card items. This is actually a worse idea than using codes, the chances of getting busted are very high.

VIII. If for some reason you have to use codes, use your own, and nothing else. Never use a code you see on a board, because chances are it has been abused beyond belief and it is already being monitored.

IX. Feel free to ask questions, but keep them within reason. People won't always be willing to hand out rare accounts, and if this is the case don't be surprised. Keep the questions technical as a rule. Try and learn as much as you can from pure hands on experience

X. And finally, be somewhat paranoid. Use PGP to encrypt your files, keep your notes/printouts stored secretly, whatever you can do to prolong your stay in the h/p world.

XI. If you get busted, don't tell the authorities ANYTHING. Refuse to speak to them without a lawyer present.

XII. If police arrive at your residence to serve a search warrant, look it over carefully, it is your right. Know what they can and can't do, and if they can't do something, make sure they don't.

XIII. If at all possible, try not to hack off your own phoneline. Splice your neighbour's line, call from a Fortress Fone, phreak off a junction box, whatever.. if you hack long enough, chances are one day you'll be traced or ANI'd.
Don't believe you are entirely safe on packet-switched networks either, it takes a while but if you scan/hack off your local access point they will put a trace on it.

XIV. Make the tracking of yourself as difficult as possible for others. Bounce the call off several outdials, or try to go through at least two different telco companies when making a call to a dialup.
When on a packet-switched network or a local or wide area network, try and bounce the call off various pads or through other networks before you reach your destination. The more bounces, the more red tape for the investigator and the easier it is for you to make a clean getaway.
Try not to stay on any system for *too* long, and alternate your calling times and dates.

XV. Do not keep written notes! Keep all information on computer, encrypted with PGP or another military-standard encryption program.
Written notes will only serve to incriminate you in a court of law.
If you write something down originally, shred the paper.. itty bitty pieces is best, or even better, burn it! Feds DO trash, just like us, and throwing out your notes complete will land in their hands, and they'll use it against you.

XVI. Finally, the day/night calling controversy. Some folks think it is a better idea to call during the day(or whenever the user would normally use his account) as to not arouse the sysadmin's suspicion of abnormal calling times, while others think it is better to call when nobody is around.
This is a tough one, as there is no real answer. If the sysadmin keeps logs(and reads over them) he will definetly think it strange that a secretary calls in at 3 am.. he will probably then look closer and find it even stranger that the secretary then grabbed the password file and proceeded to set him/herself up with a root shell.
On the other hand, if you call during the time the user would normally call, the real owner of the account may very well log in to see his name already there, or even worse be denied access because his account

is already in use.
In the end, it is down to your opinion.
And remember, when you make a decision stick to it; remember the time zone changes.

WHERE TO START

Probably the hardest period in hacking is that of when you are first starting. Finding and penetrating your first system is a major step, and can be approached in many ways. The common ways to find a system to hack are;

- UNIVERSITIES : Universities commonly have hundreds of users, many of which aren't too computer literate, which makes hacking a relatively simple chore. And security is often poor, so if you don't abuse the system too much your stay could be a long one.
  On the other hand, for a nominal fee you can usually pick up a cheap *legitimate* (now there's a concept) account. Or you could enroll in the university for a few credits, and just go until the accounts are handed out. Unfortunely, if you are caught hacking off your own account it won't be hard to trace it back to you. If you get a legimate account at first, you might be best to hack a student's account for your other-system hacking.
  The other fun part about universities is often they will provide access to a number of nets, usually including the Internet.
  Occasionally you'll have access to a PSN as well.

- CARRIER SCANNING: Carrier scanning in your LATA(Local Access Transport Area), commonly known as wardialing, was popularized in the movie War Games.
  Unfortunely, there are a few problems inherent in finding systems this way; you are limited to the systems in your area, so if you have a small town you may find very little of interest, and secondly, ANI is a problem within your own LATA, and tracing is simple, making security risks high. If you are going to hack a system within your own lata, bounce it at least once.
  There are many programs, such as ToneLoc and CodeThief (ToneLoc being superior to all in my humble opinion), which will automate this process.

- PACKET-SWITCHED NETWORKS : This is my favorite by far, as hacking on PSNs is how I learned nearly all I know. I've explored PSNs world-wide, and never ran out of systems to hack. No matter what PSN you try you will find many different, hackable systems. I will go more indepth on PSNs in the next section.

PACKET-SWITCHED NETWORKS

Intro to PSNs

First off, PSNs are also known as PSDNs, PSDCNs, PSSs and VANs to name a few. Look up the acronyms in the handy acronym reference chart<g>.

The X.25 PSNs you will hear about the most are; Sprintnet(formerly Telenet), BT Tymnet(the largest), and Datapac(Canada's largest).

All these networks have advantages and disadvantages, but i'll say this; if you are in the United States, start with Sprintnet. If you are in Canada, Datapac is for you.

The reason PSNs are so popular for hackers are many. There are literally thousands of systems on PSNs all around the world, all of which(if you have the right facilities) are free of charge for you to reach. And because of the immense size of public PSNs, it is a rare thing to ever get caught for scanning. Tracing is also a complicated matter, especially with a small amount of effort on your part to avoid a trace.

How packet-switching works

The following explanation applies for the most part to all forms of packet-switching, but is specifically about PSNs operating on the X series of protocols, such as Datapac & SprintNet, as opposed to the Internet which operates on TCP/IP. It is the same principle in essense, however.

Packet-Switched Networks are kinda complicated, but I'll attempt to simplify the technology enough to make it easy to understand.

You, the user, connect to the local public access port for your PSN, reachable via a phone dialup. You match communications parameters with the network host and you are ready to go.

From there, all the data you send across the network is first bundled into packets, usually of 128 or 256 bytes. These packets are assembled using Packet Assembly/Disassembly, performed by the public access port, also known as a public PAD(Packet Assembler/Disassembler), or a DCE(Data Communicating Equipment or Data Circuit-Terminating Equipment).

The packets are sent along the network to their destination by means of the various X protocols, standardly X.25 with help from X.28, X.29 & X.3 within your home network, and internationally using X.75/X.121. The X protocol series are the accepted CCITT standards.

The host system(DTE: Data Terminal Equipment, also a PAD) which you are calling then receives the packet and disassembles the packet using Packet Assembly/Disassembly once again into data the system understands.

The DTE then assembles it's data in response to your packet, and sends it back over the network to your PAD in packet form, which disassembles the packet into readable data for you, the user.

And that is the simplified version!

The Internet

Introduction

Contrary to popular belief, the Internet is a packet-switched network; just not an X.25 packet-switched network. The Internet operates on the TCP/IP protocols(as a rule), which is why it is sometimes disregarded as a packet-switched network. In fact, the Internet's predecessor, the ARPAnet, was the first large-scale experiment in packet-switching technology. What was then Telenet came later.

The confusion comes from peoples ignorance of the principles of packet-switching, which is simply a type of network, explained in technical detail earlier. It doesn't matter what protocols the network may use, if packet-switching is in use it is obviously a packet-switched network.

Ok, now you may have noticed that the Internet has a rather small section, which is true. The reasons are many. This is a hacking guide, not an Internet tutorial, so I didn't include the IRC or Archie or whatever. And the main reason is I spent about 100% more time on X.25 nets than I did the Internet.

Nonetheless, I decided to include the essential aspects of the Internet. You should be able to take it from there.

The following section is derived mostly from personal experience, but

the Gatsby's Internet file helped out somewhat, specifically in the classes of IP addresses.

Getting Access

Getting access is somewhere between easy and very difficult, depending where you live and how good(or lucky!) a hacker you are.

First of all, if you are going to hack on the Internet then you must be on a system that has full Internet access, not just mail. That cuts Compuserve and Prodigy out of the picture.

Most universities and some high schools have Internet access, see what you can do to get yourself an account, legitimatly or not.

Some BBSes offer full Internet access for a fairly reasonable price, and that would be a good choice.

If you are in an area with a FreeNet, then you get full Internet access.. for free! Check around with local hackers or PD boards to inquire where the nearest FreeNet is.

Some businesses provide Internet access, for a price. Check with local netters to see what local options there are.

And lastly, you can try and hack your way on. When you hack a system, check and see if they are on the net. Usually this is accomplished by doing a test call using telnet.. explained later.

FTP

FTP is the acronym for File Transfer Protocol, and it is the primary means of transporting remote files onto your own system(actually, usually the system which you are calling the Internet through).

I will only provide a brief overview, as FTP is fairly easy to use, has help files online and comprehensive documentation offline at your local h/p BBS.

First off, FTP can be initialized by typing 'ftp' at any system which has it. Most do, even if they don't have the Internet online. That a frustrating lesson more than a few novices has learned.. if you hack into a system that has FTP or telnet on line, it does not necessarily(and usually doesn't) have Internet access. Some SunOS's will have two sets of ftp and telnet utilities. The standard ftp and telnet commands can be used for local network connects, but not Internet. Another set of commands, itelnet, iftp and ifinger (and occasionally iwhois) is used for the Internet.

When you enter the FTP utility, you'll usually find yourself at a 'ftp>' prompt, and typing 'help' should bring up a small set of help files. The commands available, along with the help files, vary from system to system.

Procedure is then defined by what type of system you are on, as again, it varies. But what you usually do next is open a connection to the system you want to get a file off of. Type 'open' followed by the host name or IP address of the system you wish to connect to.. explained later.

Next, you will usually find yourself at a sort of login prompt. If you have a username on that system, then type it in. If not, try 'anonymous'. Anonymous is a great little guest account that is now being built in to some OS's. Conscientious sysadmins may disable it, for obvious reasons. If however, it is not, you will be asked for a password. Type anything, it doesn't matter really. Type a few d's if you want, it really doesn't matter(as a rule don't sit on your keyboard though.. it may not like it.. type something boring).

Next you simply use the 'get' command to get the file you want. Usually it is a good idea to not put the files in a directory that they will be noticed.. the sysadmin will suspect something is up if he runs into a few files that he supposedly copied into his own directory. Which brings us to the next segment.. give your files benign names, especially if they are something like /etc/passwd files or issues of Phrack.

A note about FTPing /etc/passwds. It rarely works. Oh yes, you will get an /etc/passwd file, but rarely on the Internet will it be the real /etc/passwd. Check the size of the file first.. if it is 300 bytes or less,

then it will likely be a substitute. Telnet will, however, get the real /etc/passwd on most occasions.

Now quit the FTP utility and peruse your new files.. be sure to remove them when done.

Telnet

While FTP has no real parallel in X.25 networks, you could equate telnet to a private PAD. Telnet lets you connect to and operate on Internet systems over the Internet as if you were connected locally.

Telnet is initialized by typing 'telnet' at your shell. The operative command is, again, 'open'. Again, type 'open' followed by the domain name or the IP address. When connected, you will be at a login prompt of some kind(usually..). Enter a username if you have one, and if not you can either attempt to hack one or see if the system accepts the 'anonymous' guest user, explained in the FTP section.

If all goes well, you should have a remote connection of some kind, and what follows depends on the system you are connected to, just like in any other network.

Domain Names and IP Addresses - Intro

For those of you unfamiliar with those terms I will give a small, condensed explanation of what the two are.

One or the other is needed for connecting to a remote system, either by FTP or Telnet. The IP address could be equated to the X.25 net's Network User Address. The Domain name is a mnemonic name, used for convience more than anything, as it is generally easier to remember.

If you wish to scan for systems on the Internet it is usually much easier to scan by IP address, as you won't know the mnemonic for most systems.

IP addresses are 4 digit-combinations separated by dots. Address examples are 192.88.144.3(EFF) and 18.72.2.1(MIT).

Addresses fall into three classes;

```
Class A  -  0 to 127
Class B  -  128 to 191
Class C  -  192 to 223
```

The earliest Internet systems are all in Class A, but it is more common to find class B or C systems. Moreover, a lot of systems are placed specifically in the 128 or 192 address prefix, as opposed to 184 or 201 or whatever. Scanning an IP address set can be accomplished in many fashions. One of which would be to pick a prefix, add two random one to two digit numbers, and scan the last portion. ie: take 192.15.43 and scan the last digit from 0 to 255.

Unfortunely, the last portion (or last two portions in the case of Class C) are ports, meaning you may come up completely blank or you might hit the jack pot.

Experiment to your own liking, after a while you will fall into a comfortable groove.

You can also connect to specific systems using the domain name, if you know or can guess the domain name. To guess a domain name you will need to know the company or organization's name, and the type of organization it is. This is possible because host names must follow the Domain Name System, which makes guessing a lot easier. Once you have both, you can usually take a few educated guesses at the domain name. Some are easier than others.

First of all, you will need to understand the principle of top-level domains. The top level is at the end of a domain name; in the case of eff.org, the top-level is 'org'. In the case of mit.edu, the top-level is 'edu'.

Top levels fall into a few categories;

```
com - commercial institutions
org - non-profit organizations
edu - educational facilities
net - networks
```

gov - government systems (non military)
mil - non-classified military

Along with various country codes. The country codes are two letters used for international calls; the US's is 'US', Brazil's is 'BR'.

Determine which top-level the system falls under, and then make a few guesses. Examples are;

compuserve.com
xerox.com
mit.edu
eff.org

For further reading, I suggest picking up a few of the printed Internet guides currently on the market, as well as the Gatsby's file on the Internet, printed in Phrack 33.

X.25 Networks

From here on in the PSN section of this file is dedicated to X.25 networks. I use the acronym PSN interchangably with X.25 networks, so don't get PSN confused with all the other types of PSN networks. From here on in, it is all X.25.

Network User Addresses

NUAs(Network User Addresses) are the PSNs equivalent of a phone number. They are what you need to connect to systems on PSNs around the world, and thanks to the DNIC(Data Network Identifier Code), there are no two the same.

The format for entering NUAs is different from PSN to PSN. For example, on Datapac you must include 0's, but on Sprintnet 0's are not necessary. Tymnet uses 6 digits NUAs rather than the standard 8.
But the standard NUA format is this;

PDDDDXXXXXXXXSS,MMMMMMMMMM

Where; P is the pre-DNIC digit
D is the DNIC
X is the NUA
S is the LCN(Logical Channel Number, subaddressing)
M is the Mnemonic

Various segments may be omitted depending on your PSN and where you are calling.
The P is commonly a 0, but is a 1 on Datapac. It is not usually even counted as part of the NUA, but must be included(usage varying) when making calls to another PSN other than your own. Within your own PSN it is not necessary to include the pre DNIC digit.
The D is the DNIC also known as the DCC(Data Country Code). The DNIC is the 4 digit country code, which insures that each NUA worldwide is unique. The DNIC is only used in calling international NUAs. If you are in Datapac(DNIC 3020) you do not have to include the DNIC for Datapac when making calls to NUAs within Datapac, but if you are in another PSN you must include the DNIC for calls to Datapac.
The X symbolizes the actual NUA, which along with the optional S (subaddressing) must always be included. You can simplify the NUA even greater using this format;

PPPXXXXX

Where P is the prefix of the NUA, and the X's are the suffix. The prefix corresponds to an Area Code in most cases in that the NUAs within that prefix are in a certain part of the country the PSN serves. In the case of Sprintnet, the prefix corresponds directly with the Area Code(ie: all NUAs in the 914 prefix on Sprintnet are in New York, and all phone numbers in the 914 Area

Code are in New York).
Subaddressing, S on the diagram, is a somewhat complicated thing to explain. Subaddressing is used when desired by the owner of the DTE, and is used to connect to specified system on the same NUA. You may find more than one system on the same NUA, and these can be reached using subaddresses.
ie:

	NUA PPPXXXXXSS	SYSTEM
Ex.1	12300456	Unix
Ex.2	123004561	VMS
Ex.3	1230045699	HP3000

In this example, the normal NUA is 12300456(assuming DNIC and pre-DNIC digit are not used). This NUA takes you to a Unix system. But when the LCN(Logical Channel Number, subaddress) of 1 is used, you are taken to a VMS. And the subaddress of 99 takes you to a HP3000. The systems on 12300456 are all owned by the same person/company, who wished to have one NUA only, but by using subaddresses he can give access to multiple systems on a lone NUA.
Subaddresses are also used occasionally as extra security. If you hit a system that gives you an error message such as 'REMOTE PROCEDURE ERROR' or 'REMOTE DIRECTIVE', you will either need a subaddress or a mnemonic. You may choose to go through the entire possible subaddresses, 1 to 99, or if you are just scanning i would suggest these: 1,2,50,51,91,98,99
Mnemonics, M, are another tricky one to explain. They are not documented by the PSNs, I discovered them on my own. Mnemonics are also used to select systems on a single NUA as a kind of port selector, but they are more commonly used as a kind of external password, which prevents you from even seeing the system in question.
The same error messages as in LCNs occur for mnemonics, but again, even if you can reach a system with a standard NUA, there is a possibly a system only reachable by mnemonic exists. Here is a list of commonly used mnemonics;
    SYSTEM CONSOLE PAD DIAL MODEM X25 X28 X29 SYS HOST

Bypassing Reverse Charging Systems: Private PADs and NUIs

    Occasionally on PSNs you will run into systems which give you the error message 'COLLECT CALL REFUSED'. This denotes a reverse-charging system. When you make a call to a system on a PSN, the call is automatically collect. But a lot of sysadmins do not want to pay for your connect charges, and if all of their users have NUIs or private PADs, it is a good idea for them to make their system reverse-charging, which saves them money, but also acts as yet another security barrier from casual snoopers.
    But again, this can be avoided by using a private PAD or a NUI.
Before we go into the details of these, remember that a private PAD is a different thing than your public access port PAD. A private PAD is a PAD which automatically assumes all connect charges. So, the reverse charging systems will let you past the reverse charging, as you agree to accept the charges.
    NUI's(Network User Identifiers) work the same way. You can think of a NUI as .. say a Calling Card. The Calling Card is billed for all the charges made on it, regardless of who made them; the owner gets the bill. The NUI works the same way. NUIs are used legitimatly by users willing to accept the connect charges. But, as hackers are known to do, these NUIs get stolen and used to call all NUAs all around the world, and the legitimate owner gets the bill. But unlike CCs, you will usually get away with using a NUI.
    However, as you can guess, private PADs and NUIs are fairly hard to come by. If somebody manages to get ahold of one, they usually won't be willing to share it. So, it comes down to you; you probably will have to find your own.
    PADs are only found by scanning on PSNs, and by hacking onto systems on PSNs. There are programs on Unix and Primos systems,for example, that serve as a private PAD. And there are some private PADs that are set up solely for the purpose of being a private PAD. But, these are almost always passworded, so it is up to you to get in.

NUIs are somewhat the same thing. NUIs are different from PSN to PSN, some will tell you if a NUI is wrong, letting you guess one, but others will not. And of course, you still have to guess the password. I've heard stories of people carding NUIs, but i'm not sure i quite believe it, and the safety of such a practice is questionable.

Closed User Groups

One of the most effective security measures i've ever seen is the CUG (Closed User Group). The CUG is what generates the 'CALL BLOCKED' message when scanning on PSNs. A CUG will only accept calls into the DTE from specified DCE NUAs. Meaning, if your NUA has not been entered into the list of acceptable NUAs, you won't be allowed to even see the system. However, CUGs aren't for everybody. If you have a system with many users that all call in from different points, CUGs are unusable. And a good thing for us. I've never heard of anyone finding a way past a CUG. I've got a few theories but..

Sprintnet

Now i'll go a bit more into the major US and Canadian PSNs, starting with the most popular in the States, Sprintnet

To find a public indial port for Sprintnet you may possibly be able to find it in your telefone book(look under Sprintnet) or by Directory Assistance. If not, try Sprintnet Customer Service at 1-800-336-0437. This also will probably only function between 8:30 and 5:00 EST, maybe a bit different.

Also, for a data number for in-dial look ups try 1-800-424-9494 at communication parameters 7/E/1(or 8/N/1 also i believe). Type <CR> twice or @D for 2400bps and press enter so Sprintnet can match your communications parameters. It will display a short herald then a TERMINAL= prompt.
At the TERMINAL= prompt type VT100 for VT100 terminal emulation, if you are using a personal computer i think D1 works, or just <CR> for dumb terminal. Then type "c mail", at the username prompt type "phones", and for password type "phones" again. It is menu driven from there on.

Now that you have your Sprintnet public dial port number, call it up like you would a BBS, then when it connnects type the two <CR>s for 300/1200bps or the @D for 2400bps, then it will display its herald, something like:

```
SPRINTNET(or in some cases TELENET)
123 11A  (where 123 is your area code & Sprintnet's address prefix
          and 11A is the port you are using)
TERMINAL=(type what you did previously eg:VT100,D1,<ENTER>)
```

then when Sprintnet displays the @ prompt you know you are connected to a Sprintnet public PAD and you are ready to enter NUAs.

As i mentioned before, Sprintnet NUA prefixes correspond directly with Area Codes, so to scan Sprintnet simply take an AC and suffix it with the remaining digits, usually in sequence. Since Sprintnet ignores 0's, NUAs can be as small as 4 digits. When scanning, go from lowest to highest, stopping as soon as it seems NUAs have run dry(take it a hundred NUAs further to be sure..best to take it right to 2000, maybe higher if you have time).

BT Tymnet

BT Tymnet is owned by British Telecom, and is the biggest PSN by far, but it does have some extra security.

For finding Tymnet dial-ins the procedure is much the same, look in the phone book under Tymnet or BT Tymnet, or phone directory assistance and ask for BT Tymnet Public Dial Port numbers, or you can call Tymnet customer Service at 1-800-336-0149. Generally try between 8:30 and 5:00 EST. I don't have the Tymnet data number for finding in-dials, but once you are on Tymnet type INFORMATION for a complete list of in-dials as well as other things.

Once you have your in-dial number set your communication parameters at either 8/N/1 or 7/E/1 then dial the number just like you would a BBS. At connect you will see a string of garbage characters or nothing at all. Press <CR> so Tymnet can match your communication parameters. You will then see the Tymnet herald which will look something like this:

```
-2373-001-
please type your terminal identifier
```

If it wants a terminal identifier press A(if you want, you can press A instead of <CR> at connect so it can match your communication parameters and get your terminal identifer all at once).

After this initial part you will see the prompt:

```
please log in:
```

This shows Tymnet is ready for you to enter NUAs. A great deal of the NUAs on Tymnet are in plain mnemonic format however. To reach these, just enter the mnemonic you wish, nothing else(ie: CPU or SYSTEM). To enter digital NUAs you need a NUI though. Tymnet will let you know when a NUI is wrong. Just keep guessing NUIs and passwords until you find one. BUT, keep in mind, one of the biggest security features Tymnet has is this: it will kick you off after three incorrect attempts at anything. Thus, you'll have to call again and again, and if you are in a digital switching system such as ESS it is not a good idea to call anywhere an excessive amount of time. So keep it in moderation if you choose to try Tymnet.

Datapac

I am the most fond of Datapac, because I grew up on it. Nearly all the hacking i've done to this day was on Datapac or the international PSNs i've been able to reach through private PADs i've found on Datapac.

To connect to the Datapac network from Canada you will need to dial into your local Datapac node, which is accessible in most cities via your local Datapac dial-in number.

There are quite a few ways to find your local Datapac dial-in. It will usually be in your telephone book under "DATAPAC PUBLIC DIAL PORT". If not, you could try directory assistance for the same name. Alternatively, there are a couple phone #'s for finding your dial port(these are also customer assistance):

```
1-800-267-6574  (Within Canada)
1-613-781-6798
```

Also, these numbers function only from 8:30 to 5:00 EST(Eastern Standard Time).Also, the Datapac Information Service(DIS) at NUA 92100086 has a complete list of all public dial-ins.

I think you can use both communication parameter settings work, but 8/N/1 (8 data bits, No parity, 1 stop bit) is used most frequently, so set it initially at that. Some NUA's on Datapac use 7/E/1, change to it if needed after you are connected to a Datapac dial-in.

Ok,if you have your Datapac 3000 Public Indial number, you've set your communication parameters at 8/N/1, then you are now set to go. Dial your indial just like a BBS(duh..) and once connnected:
You will have a blank screen;
Type 3 periods and press RETURN (this is to tell Dpac to initialize itself)
The Datapac herald will flash up stating:
DATAPAC : XXXX XXXX (your in-dial's NUA)
You are now ready to enter commands to Datapac.

Example:

```
(YOU ENTER)          atdt 16046627732
(YOU ENTER)          ...
(DATAPAC RESPONDS)   DATAPAC : 6710 1071
```

Now you are all set to enter the NUA for your destination.
NUAs on Datapac must be 8 to 10 digits(not including mnemonics).

8 is standard, but 9 or 10 is possible depending on usage of subaddressing. NUA prefixes on Datapac are handed out in blocks, meaning they do not correspond to Area Codes, but by looking at the surrounding prefixes, you can tell where a prefix is located. When scanning on Datapac, keep in mind most of the valid NUAs are found in the low numbers, so to sample a prefix go from (example) 12300001 to 12300200. It is a good idea, however, to scan the prefix right up until 2000, the choice is yours.

DNIC List

Here is a list of the previous PSN's DNICs, and most of the other DNICs for PSNs world wide. This was taken from the DIS, with a number of my own additions that were omitted(the DIS did not include other Canadian or American PSNs). The extras DNICs came from my own experience and various BBS lists.

COUNTRY	NETWORK	DNIC	DIRECTION
ANDORRA	ANDORPAC	2945	BI-DIR
ANTIGUA	AGANET	3443	INCOMING
ARGENTINA	ARPAC	7220	BI-DIR
	ARPAC	7222	BI-DIR
AUSTRIA	DATEX-P	2322	BI-DIR
	DATEX-P TTX	2323	BI-DIR
	RA	2329	BI-DIR
AUSTRALIA	AUSTPAC	5052	BI-DIR
	OTC DATA ACCESS	5053	BI-DIR
AZORES	TELEPAC	2680	BI-DIR
BAHAMAS	BATELCO	3640	BI-DIR
BAHRAIN	BAHNET	4263	BI-DIR
BARBADOS	IDAS	3423	BI-DIR
BELGIUM	DCS	2062	BI-DIR
	DCS	2068	BI-DIR
	DCS	2069	BI-DIR
BELIZE	BTLDATAPAC	7020	BI-DIR
BERMUDA	BERMUDANET	3503	BI-DIR
BRAZIL	INTERDATA	7240	BI-DIR
	RENPAC	7241	BI-DIR
	RENPAC	7248	INCOMING
	RENPAC	7249	INCOMING
BULGARIA	BULPAC	2841	BI-DIR
BURKINA FASO	BURKIPAC	6132	BI-DIR
CAMEROON	CAMPAC	6242	BI-DIR
CANADA	DATAPAC	3020	BI-DIR
	GLOBEDAT	3025	BI-DIR
	CNCP PACKET NET	3028	BI-DIR
	CNCP INFO SWITCH	3029	BI-DIR
CAYMAN ISLANDS	IDAS	3463	BI-DIR
CHAD	CHADPAC	6222	BI-DIR
CHILE	ENTEL	7302	BI-DIR
	CHILE-PAC	7303	INCOMING
	VTRNET	7305	BI-DIR
	ENTEL	7300	INCOMING
CHINA	PTELCOM	4600	BI-DIR
COLOMBIA	COLDAPAQ	7322	BI-DIR
COSTA RICA	RACSAPAC	7120	BI-DIR
	RACSAPAC	7122	BI-DIR
	RACSAPAC	7128	BI-DIR
	RACSAPAC	7129	BI-DIR
CUBA	CUBA	2329	BI-DIR
CURACAO	DATANET-1	3621	BI-DIR
CYPRUS	CYTAPAC	2802	BI-DIR

	CYTAPAC	2807	BI-DIR
	CYTAPAC	2808	BI-DIR
	CYTAPAC	2809	BI-DIR
DENMARK	DATAPAK	2382	BI-DIR
	DATAPAK	2383	BI-DIR
DJIBOUTI	STIPAC	6382	BI-DIR
DOMINICAN REP.	UDTS-I	3701	INCOMING
EGYPT	ARENTO	6020	BI-DIR
ESTONIA	ESTPAC	2506	BI-DIR
FIJI	FIJIPAC	5420	BI-DIR
FINLAND	DATAPAK	2441	BI-DIR
	DATAPAK	2442	BI-DIR
	DIGIPAK	2443	BI-DIR
FRANCE	TRANSPAC	2080	BI-DIR
	NTI	2081	BI-DIR
	TRANSPAC	2089	BI-DIR
	TRANSPAC	9330	INCOMING
	TRANSPAC	9331	INCOMING
	TRANSPAC	9332	INCOMING
	TRANSPAC	9333	INCOMING
	TRANSPAC	9334	INCOMING
	TRANSPAC	9335	INCOMING
	TRANSPAC	9336	INCOMING
	TRANSPAC	9337	INCOMING
	TRANSPAC	9338	INCOMING
	TRANSPAC	9339	INCOMING
FR ANTILLIES	TRANSPAC	2080	BI-DIR
FR GUIANA	TRANSPAC	2080	BI-DIR
FR POLYNESIA	TOMPAC	5470	BI-DIR
GABON	GABONPAC	6282	BI-DIR
GERMANY F.R.	DATEX-P	2624	BI-DIR
	DATEX-C	2627	BI-DIR
GREECE	HELPAK	2022	BI-DIR
	HELLASPAC	2023	BI-DIR
GREENLAND	KANUPAX	2901	BI-DIR
GUAM	LSDS-RCA	5350	BI-DIR
	PACNET	5351	BI-DIR
GUATEMALA	GUATEL	7040	INCOMING
	GUATEL	7043	INCOMING
HONDURAS	HONDUTEL	7080	INCOMING
	HONDUTEL	7082	BI-DIR
	HONDUTEL	7089	BI-DIR
HONG KONG	INTELPAK	4542	BI-DIR
	DATAPAK	4545	BI-DIR
	INET HK	4546	BI-DIR
HUNGARY	DATEX-P	2160	BI-DIR
	DATEX-P	2161	BI-DIR
ICELAND	ICEPAK	2740	BI-DIR
INDIA	GPSS	4042	BI-DIR
	RABMN	4041	BI-DIR
	I-NET	4043	BI-DIR
INDONESIA	SKDP	5101	BI-DIR
IRELAND	EIRPAC	2721	BI-DIR
	EIRPAC	2724	BI-DIR
ISRAEL	ISRANET	4251	BI-DIR
ITALY	DARDO	2222	BI-DIR
	ITAPAC	2227	BI-DIR
IVORY COAST	SYTRANPAC	6122	BI-DIR
JAMAICA	JAMINTEL	3380	INCOMING
JAPAN	GLOBALNET	4400	BI-DIR
	DDX	4401	BI-DIR
	NIS-NET	4406	BI-DIR
	VENUS-P	4408	BI-DIR
	VENUS-P	9955	INCOMIMG

	VENUS-C	4409	BI-DIR
	NI+CI	4410	BI-DIR
KENYA	KENPAC	6390	BI-DIR
KOREA REP	HINET-P	4500	BI-DIR
	DACOM-NET	4501	BI-DIR
	DNS	4503	BI-DIR
KUWAIT	BAHNET	4263	BI-DIR
LEBANON	SODETEL	4155	BI-DIR
LIECHTENSTEIN	TELEPAC	2284	BI-DIR
	TELEPAC	2289	BI-DIR
LUXEMBOURG	LUXPAC	2704	BI-DIR
	LUXPAC	2709	BI-DIR
MACAU	MACAUPAC	4550	BI-DIR
MADAGASCAR	INFOPAC	6460	BI-DIR
MADEIRA	TELEPAC	2680	BI-DIR
MALAYSIA	MAYPAC	5021	BI-DIR
MAURITIUS	MAURIDATA	6170	BI-DIR
MEXICO	TELEPAC	3340	BI-DIR
MOROCCO	MOROCCO	6040	BI-DIR
MOZAMBIQUE	COMPAC	6435	BI-DIR
NETHERLANDS	DATANET-1	2040	BI-DIR
	DATANET-1	2041	BI-DIR
	DABAS	2044	BI-DIR
	DATANET-1	2049	BI-DIR
N. MARIANAS	PACNET	5351	BI-DIR
NEW CALEDONIA	TOMPAC	5460	BI-DIR
NEW ZEALAND	PACNET	5301	BI-DIR
NIGER	NIGERPAC	6142	BI-DIR
NORWAY	DATAPAC TTX	2421	BI-DIR
	DATAPAK	2422	BI-DIR
	DATAPAC	2423	BI-DIR
PAKISTAN	PSDS	4100	BI-DIR
PANAMA	INTELPAQ	7141	BI-DIR
	INTELPAQ	7142	BI-DIR
PAPUA-NEW GUINEA	PANGPAC	5053	BI-DIR
PARAGUAY	ANTELPAC	7447	BI-DIR
PERU	DICOTEL	7160	BI-DIR
PHILIPPINES	CAPWIRE	5150	INCOMING
	CAPWIRE	5151	BI-DIR
	PGC	5152	BI-DIR
	GLOBENET	5154	BI-DIR
	ETPI	5156	BI-DIR
POLAND	POLAK	2601	BI-DIR
PORTUGAL	TELEPAC	2680	BI-DIR
	SABD	2682	BI-DIR
PUERTO RICO	UDTS	3300	BI-DIR
	UDTS	3301	BI-DIR
QATAR	DOHPAC	4271	BI-DIR
REUNION (FR)	TRANSPAC	2080	BI-DIR
RWANDA	RWANDA	6352	BI-DIR
SAN MARINO	X-NET	2922	BI-DIR
SAUDI ARABIA	ALWASEED	4201	BI-DIR
SENEGAL	SENPAC	6081	BI-DIR
SEYCHELLES	INFOLINK	6331	BI-DIR
SINGAPORE	TELEPAC	5252	BI-DIR
	TELEPAC	5258	BI-DIR
SOLOMON ISLANDS	DATANET	5400	BI-DIR
SOUTH AFRICA	SAPONET	6550	BI-DIR
	SAPONET	6551	BI-DIR
	SAPONET	6559	BI-DIR
SPAIN	TIDA	2141	BI-DIR
	IBERPAC	2145	BI-DIR
SRI-LANKA	DATANET	4132	BI-DIR
SWEDEN	DATAPAK TTX	2401	BI-DIR

	DATAPAK-2	2403	BI-DIR
	DATAPAK-2	2407	BI-DIR
SWITZERLAND	TELEPAC	2284	BI-DIR
	TELEPAC	2285	BI-DIR
	TELEPAC	2289	BI-DIR
TAIWAN	PACNET	4872	BI-DIR
	PACNET	4873	BI-DIR
	UDAS	4877	BI-DIR
TCHECOSLOVAKA	DATEX-P	2301	BI-DIR
THAILAND	THAIPAC	5200	BI-DIR
	IDAR	5201	BI-DIR
TONGA	DATAPAK	5390	BI-DIR
TOGOLESE REP.	TOGOPAC	6152	BI-DIR
TORTOLA	IDAS	3483	INCOMING
TRINIDAD	DATANETT	3745	BI-DIR
	TEXTET	3740	BI-DIR
TUNISIA	RED25	6050	BI-DIR
TURKEY	TURPAC	2862	BI-DIR
	TURPAC	2863	BI-DIR
TURKS&CAICOS	IDAS	3763	INCOMING
U ARAB EMIRATES	EMDAN	4241	BI-DIR
	EMDAN	4243	BI-DIR
	TEDAS	4310	INCOMING
URUGUAY	URUPAC	7482	BI-DIR
	URUPAC	7489	BI-DIR
USSR	IASNET	2502	BI-DIR
U.S.A.	WESTERN UNION	3101	BI-DIR
	MCI	3102	BI-DIR
	ITT/UDTS	3103	BI-DIR
	WUI	3104	BI-DIR
	BT-TYMNET	3106	BI-DIR
	SPRINTNET	3110	BI-DIR
	RCA	3113	BI-DIR
	WESTERN UNION	3114	BI-DIR
	DATAPAK	3119	BI-DIR
	PSTS	3124	BI-DIR
	UNINET	3125	BI-DIR
	ADP AUTONET	3126	BI-DIR
	COMPUSERVE	3132	BI-DIR
	AT&T ACCUNET	3134	BI-DIR
	FEDEX	3138	BI-DIR
	NET EXPRESS	3139	BI-DIR
	SNET	3140	BI-DIR
	BELL SOUTH	3142	BI-DIR
	BELL SOUTH	3143	BI-DIR
	NYNEX	3144	BI-DIR
	PACIFIC BELL	3145	BI-DIR
	SWEST BELL	3146	BI-DIR
	U.S. WEST	3147	BI-DIR
	CENTEL	3148	BI-DIR
	FEDEX	3150	BI-DIR
U.S. VIRGIN I	UDTS	3320	BI-DIR
U. KINGDOM	IPSS-BTI	2341	BI-DIR
	PSS-BT	2342	BI-DIR
	GNS-BT	2343	BI-DIR
	MERCURY	2350	BI-DIR
	MERCURY	2351	BI-DIR
	HULL	2352	BI-DIR
VANUATU	VIAPAC	5410	BI-DIR
VENEZUELA	VENEXPAQ	7342	BI-DIR
YUGOSLAVIA	YUGOPAC	2201	BI-DIR
ZIMBABWE	ZIMNET	6484	BI-DIR

SYSTEM PENETRATION

Ok, now that you've hopefully found some systems, you are going to need to know how to identify and, with any luck, get in these newfound delights.

What follows is a list of as many common systems as i could find. The accounts listed along with it are not, per say, 'defaults'. There are very few actual defaults. These are 'common accounts', in that it is likely that many of these will be present. So, try them all, you might get lucky.

The list of common accounts will never be complete, but mine is fairly close. I've hacked into an incredible amount of systems, and because of this I've been able to gather a fairly extensive list of common accounts.

Where I left the password space blank, just try the username(and anything else you want), as there are no common passwords other than the username itself.

And also, in the password space I never included the username as a password, as it is a given in every case that you will try it.

And remember, passwords given are just guidelines, try what you want.

UNIX- Unix is one of the most widespread Operating Systems in the world; if you scan a PSN, chances are you'll find a number of Unixes, doesn't matter where in the world the PSN resides.
The default login prompt for a unix system is 'login', and while that cannot be changed, additional characters might be added to preface 'login', such as 'rsflogin:'. Hit <CR> a few times and it should disappear.
Because UNIX is a non-proprietary software, there are many variants of it, such as Xenix, SCO, SunOS, BSD, etc.., but the OS stays pretty much the same.
As a rule, usernames are in lowercase only, as are passwords, but Unix is case sensitive so you might want to experiment if you aren't getting any luck.
You are generally allowed 4 attempts at a login/password, but this can be increased or decreased at the sysadmins whim.
Unfortunely, UNIX does not let you know when the username you have entered is incorrect.
UNIX informs the user of when the last bad login attempt was made, but nothing more. However, the sysadmin can keep logs and audit trails if he so wishes, so watch out.
When inside a UNIX, type 'cat /etc/passwd'. This will give you the list of usernames, and the encrypted passwords.
The command 'who' gives a list of users online.
'Learn' and 'man' bring up help facilities.
Once inside, you will standardly receive the prompt $ or % for regular users, or # for superusers.
The root account is the superuser, and thus the password could be anything, and is probably well protected. I left this blank, it is up to you. There won't be any common passwords for root.

COMMON ACCOUNTS:

Username	Password
root	
daemon	
adm	admin, sysadm, sysadmin, operator, manager
uucp	
bin	
sys	
123	lotus, lotus123
adduser	
admin	adm,sysadm,sysadmin,operator,manager

anon	anonymous
anonuucp	anon, uucp, nuucp
anonymous	anon
asg	device devadmin
audit	
auth	
backappl	
backup	save, tar
batch	
bbx	
blast	
bupsched	
cbm	
cbmtest	
checkfsys	
control	
cron	
csr	support, custsup
dbcat	database, catalog
default	user, guest
demo	tour, guest
dev	
devel	
devshp	
diag	sysdiag, sysdiags, diags, test
diags	diag, sysdiag, sysdiags
dialup	
dos	
fax	
field	fld, service, support, test
filepro	
finger	
fms	
friend	guest, visitor
games	
general	
gp	
gsa	
guest	visitor, demo, friend, tour
help	
host	
hpdb	
info	
informix	database
ingres	database
inquiry	
install	
journal	
journals	
kcml	
learn	
lib	library, syslib
link	
listen	
lp	print spooler lpadmin
lpadmin	lp, adm, admin
lpd	
ls	
mail	
maint	sysmaint, service
makefsys	
man	
manager	mgr, man, sysmgr, sysman, operator
mdf	

menu	
mountfsys	
ncrm	ncr
net	network
netinst	inst, install, net, network
netman	net, man, manager, mgr, netmgr, network
netmgr	net, man, manager, mgr, netmgr, network
network	net
newconv	
news	
nobody	anon
nuucp	anon
oasys	oa
odt	opendesktop
online	
openmail	mail
oper	operator,manager,adm,admin,sysadmin,mgr
operator	sysop, oper, manager
opp	
oracle	database
oraclev5	oracle, database
oradev	oracle
pcs	
pcsloc	
pctest	
postmaster	mail
powerdown	shutdown
priv	private
prod	
pub	public
public	pub
reboot	
remote	
report	
rha	
rje	
rsm	
rsmadm	rsm, adm, admin
rusr	
sales	
sas	
save	backup
savep	
service	field, support
setup	
shutdown	
smtp	mail
softwork	
space	
startup	
su	
sundiag	sysdiag, diag, diags, sysdiags
suoper	su, oper, operator
super	supervisor, manager, operator
support	field, service
sync	
sysadm	adm, admin, operator, manager
sysdiag	diag, diags, sysdiags
sysinfo	info
sysmaint	maint, service
sysman	manager,mgr,man,admin,operator,sysadmin
sysmgr	manager,mgr,man,admin,operator,sysadmin
system	sys, unix, shell, syslib, lib, operator
systest	test, tester, testuser, user

test	tester, testuser, systest, user
tester	test, user, testuser
testuser	test, tester, user, systest
tftp	
tour	demo, guest, user, visitor
transfer	
tty	
tutor	
tutorial	
umountfsys	
unix	
unixmail	mail, unix
user	guest, demo
userp	user
usr	user
usrlimit	
utest	
uucpadm	adm, admin, uucp
uuadm	uucp, adm
uuadmin	uucp, admin
uuhost	uucp, host
uulog	uucp, log
uunx	uucp
uupick	uucp, pick
uustat	uucp, stat
uuto	uucp, to
uux	uucp
va	
vashell	
vax	
visitor	guest, friend, demo, tour
vlsi	
vmsys	vm, face
vsifax	
who	
wp	
wp51	
x25	pad
x25test	test
x400	

VMS- DEC's Virtual Memory System commonly runs on VAX computers. It is another very widespread system, with many users world wide.
VMS will have a 'Username:' prompt, and to be sure just type in a ',' for a username. A VMS will throw back an error message on special delimeters.
You will standardly get 3 and only three login attempts, and VMS is not kind enough to let you know when you have entered an incorrect username.
Once inside you will find yourself at a $ prompt.

COMMON ACCOUNTS:

Username	Password
backup	
batch	
dcl	
dec	
decmail	mail
decnet	
default	default, user
dialup	

demo	guest
dsmmanager	dsm, manager
dsmuser	dsm, user
field	field, service, support, test, digital
games	
guest	visitor, demo
help	
helpdesk	
help_desk	helpdesk
host	
info	
ingres	database
interactive	
link	
local	
mail	
mailer	mail
mbmanager	mb, manager, mgr, man
mbwatch	watch, mb
mpdbadmin	mpdb, admin
netcon	net, network
netmgr	net, manager, mgr, operator
netpriv	network, private, priv, net
netserver	
network	net
newingres	ingres
news	
operations	operations
operator	oper, manager, mgr, admin,
opervax	operator, vax
ops	
oracle	
pcsdba	
pfmuser	pfm, user
postmaster	mail
priv	private
remote	
report	
rje	remote, job, entry
student	
suggest	suggest
sys	
sysmaint	sysmaint, maint, service, digital
system	manager,operator,sys,syslib
systest	uetp,test
systest_clig	systest, test
tapelib	
teledemo	demo
test	testuser, tester
uetp	
user	test, guest, demo
userp	user
vax	
vms	
visitor	guest, demo
wpusers	

HP3000- HP3000 mainframes run the MPE series of operating systems, such as MPE, V, ix, X, and XL.
The default login prompt is ':', but this can be prefaced with characters(ie: 'mentor:') and in some cases the ':' may be taken completely away (ie: 'mentor'). To check for a HP3000, hit a <CR>, you will get an error message such as this;
EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON. (CIERR 1402)

To login type 'hello', followed by the login information, which is in this format: USER.ACCOUNT,GROUP.
The group is optional, but may be needed in some cases, and can give you different file sets and the sort.
A great thing about HP3000's is they tell you exactly what is incorrect about the login name you've supplied them, be it the account is valid but the username is wrong, or the other way around.
But unfortunely, if the system operators choose, they may password ALL of the login name segments; username, account and group.
The internal prompt for MPE's is, again, :.
'Help' will give you help when inside a HP3000.
When entering accounts, i'd suggest not to use a group at first. If you receive the error message 'not in home group', then try the group PUB, then if even that fails, move on to the common group list.
I didn't list passwords along with the accounts, as it would be a bit of an awkward format, because of MPE's awkward format. The only manufacturer default passwords I am aware of are 'hponly', for mgr.telesup, 'lotus', for mgr.sys, and 'hpword' for field.support.
Just remember to try the various parts of the account as a password, and anything else along those lines.
If you need a password for the following user.accounts & groups, try the various parts of the name plus any combinations of it or names with obvious links to it(ie: field=service).

COMMON ACCOUNTS:

Username.Account
---
mgr.3000devs
mgr.acct
mgr.backup
manager.blast
manager.blast1
mgr.ccc
spool.ccc
mgr.cnas
manager.cognos
mgr.cognos
operator.cognos
mgr.common
mgr.company
mgr.conv
mgr.corp
mgr.cslxl
mgr.demo
operator.disc
mgr.easy
mgr.easydev
mgr.extend
mgr.hpdesk
mgr.hplanmgr
field.hpncs
mgr.hpncs
advmail.hpoffice
deskmon.hpoffice
mail.hpoffice
mailman.hpoffice
mailroom.hpoffice
mailtrck.hpoffice

manager.hpoffice
mgr.hpoffice
openmail.hpoffice
pcuser.hpoffice
spoolman.hpoffice
x400fer.hpoffice
x400xfer.hpoffice
wp.hpoffice
mgr.hponly
mgr.hpoptmgt
field.hpp187
mgr.hpp187
mgr.hpp189
mgr.hpp196
mgr.hppl85
mgr.hppl87
mgr.hppl89
mgr.hppl96
mgr.hpskts
mgr.hpspool
mgr.hpword
mgr.hpx11
dpcont.hq
mgr.hq
mgr.indhpe
mgr.infosys
mgr.intx3
manager.itf3000
mail.mail
mgr.netbase
mgr.netware
operator.netware
mgr.orbit
mgr.prod
mgr.rego
mgr.remacct
mgr.rje
manager.security
mgr.security
mgr.sldemo
mgr.snads
mgr.softrep
mgr.speedwre
mgr.spool
manager.starbase
field.support
mgr.support
operator.support
exploit.sys
manager.sys
mgr.sys
operator.sys
pcuser.sys
rsbcmon.sys
operator.syslib
sysrpt.syslib
mgr.sysmgr
operator.system
mgr.tech
mgr.techxl
mgr.telamon
field.hpword
mgr.opt
manager.tch

field.telesup
mgr.telesup
sys.telesup
mgr.tellx
monitor.tellx
mgr.utility
mgr.vecsl
manager.vesoft
mgr.vesoft
mgr.word
field.xlserver
mgr.xlserver
mgr.xpress

COMMON GROUPS:

admin
advmail
ask
brwexec
brwonlne
brwspec
bspadmin
bspdata
bspinstx
bsptools
catbin1
catbin2
catlib
classes
config
console
convert
creator
curator
currarc
current
dat
data
database
delivery
deskmon
devices
diadb
diag
diafile
diaipc
doc
docxl
document
dsg
easy
ems
emskit
etdaemon
example
examples
ezchart
galpics
graphics
hold
hpaccss
hpadvlk
hpadvml

hpdesk
hpdraw
hpecm
hpemm
hpenv
hpgal
hphpbkp
hplibry
hplist
hplt123
hpmail
hpmap
hpmenu
hpprofs
hpsw
hptelex
ibmpam
idl
idlc
idpxl
include
infoxl
instx
internal
itpxl
job
lib
libipc
library
mailconf
maildb
mailhelp
mailjob
maillib
mailserv
mailstat
mailtell
mailxeq
mediamgr
memo
memory
mgr
mmgrdata
mmgrxfer
mmordata
mmorxfer
monitor
mpexl
ndfiles
ndports
net
network
nwoconf
office
oldmail
oper
operator
out
pascalc
patchxl
pcbkp
ppcdict
ppcsave
ppcutil

prntmate
prog
prvxl
pub
pubxl
qedit
ref
request
restore
sample
sbase
sfiles
signal
sleeper
snax25
sql
sruntime
subfile
suprvisr
sx
sys
sysmgr
sysvol
tdpdata
telex
telexjob
text
tfm
ti
tools
transmit
user
users
validate
viewlib
visicalc
wp
wp3
x400data
x400db
x400fer
x400file
xspool

VM/CMS- The VM/CMS Operating System is found on IBM mainframes, and while there are quite a few out there, they are commonly left alone by hackers who prefer Unix or VMS.
VM/CMS systems are commonly found gated off Sim3278 VTAMs and ISM systems as well.
The login prompt for CMS is '.', but additional information might be given before the prompt, such as;

```
     Virtual Machine/System Product
     !
     .
```

or;

```
     VM/370
     !
     .
```

and frequently over to the side;

```
     LOGON userid
     DIAL userid
     MSG userid message
     LOGOFF
```

but they all represent a VM/CMS system.

To logon, type 'logon' followed by the username, which is usually 1 to 8 characters in length.
To be sure it is a CMS, type 'logon' followed by some random garbage. If it is a VM/CMS, it will reply;

```
      Userid not in CP directory
```

This is one of the great things about CMS, it tells you if the login ID you entered is incorrect, thus making the finding of valid ones fairly easy.
One thing to watch out for.. if you attempt brute forcing some systems will simply shut the account or even the login facility for some time. If that is the case, find out the limit and stay just underneath it.. drop carrier or clear the circuit if necessary, but if you continually shut down the login facilities you will raise a few eyebrows before you even make it inside.
Once inside, typing 'help' will get you a moderate online manual.

COMMON ACCOUNTS

Username	Password
$aloc$	
admin	operator, manager, adm, sysadmin, sysadm
alertvm	alert
ap2svp	
apl2pp	
autolog1	autolog
autolog2	autolog
batch	
batch1	batch
batch2	batch
botinstl	
ccc	
cms	
cmsbatch	cms, batch, batch1
cmsuser	cms, user
cpms	
cpnuc	
cprm	
cspuser	user, csp
cview	
datamove	
demo1	demo
demo2	demo
direct	
dirmaint	dirmaint1
diskcnt	
entty	
erep	
formplus	
fsfadmin	fsf, adm, sysadmin, sysadm, admin, fsfadm
fsftask1	
fsftask2	
gcs	
gcsrecon	
idms	
idmsse	
iips	
infm-mgr	infm, man, manager, mgr
inoutmgr	mgr, manager
ipfappl	
ipfserv	
ispvm	

	ivpm1	
	ivpm2	
	maildel	
	mailman	
	maint	service
	moeserv	
	netview	network, view, net, monitor
	oltsep	
	op1	
	opbackup	backup
	operatns	op, operator, manager, admin
	operator	op, operatns, manager, admin
	opserver	
	pdm470	
	pdmremi	
	peng	
	presdbm	dbm
	procal	
	prodbm	prod
	promail	
	psfmaint	maint
	pssnews	news
	pvm	
	router	
	rscs	
	rscsv2	
	savsys	
	sfcm1	sfcm
	sfcntrl	
	sim3278	
	smart	
	sna	
	sqldba	database
	sqluser	user, sql
	syncrony	
	sysadmin	admin, adm, sysadm, manager, operator
	sysckp	
	sysdump1	sysdump
	syserr	
	syswrm	
	tdisk	disk, temp
	temp	
	tsafvm	
	vastest	test
	vm3812	
	vmarch	
	vmasmon	
	vmassys	
	vmbackup	backup
	vmbsysad	
	vmmap	map
	vmtape	tape
	vmtest	test, testuser
	vmtlibr	
	vmutil	util, utils
	vseipo	
	vsemaint	maint
	vseman	
	vsm	
	vtam	
	vtamuser	user, vtam
	x400x25	

PRIMOS- Run on the Prime company's mainframes, the Primos Operating

System is in fairly wide use, and is commonly found on Packet-Switched Networks worldwide.
Upon connect you will get a header somewhat like

```
     PRIMENET 23.3.0 INTENG
```

This informs you that it is indeed a Primos computer, the version number, and the system identifier the owner picked, which is usually the company name or the city the Primos is located in. If you find a Primos on a network, you will receive the Primenet header, but if it is outside of a network, the header may be different(ie:Primecon).
Hit a number of <CR>'s, and Primos will throw you the login prompt 'ER!'.
At this point, type 'login' followed by your username.
If hitting <CR>'s did not provoke an 'ER!', then type 'login' followed by your username.
If you are blessed and you find some stone age company running 18.0.0 or below, you are guaranteed access.
Just find a username and there will be no password prompt.
If for some reason passwording exists, a a few control-C's should drop you in.
Unfortunely, Primos almost always allows one and one attempt only at a username/password combination before it kicks you off, and Primos will not tell you if the ID you've entered is invalid.
Once you are inside, you will find yourself at the prompt 'OK'.
'help' brings up a so-so online help guide.

COMMON ACCOUNTS

Username	Password
backup	
backup_terminal	
batch_service	
batch	
bootrun	
cmdnc0	
demo	
diag	
dos	
dsmsr	dsm
dsm_logger	dsm
fam	
games	
guest	
guest1	guest
lib	
libraries	
login_server	
mail	
mailer	
netlink	net, primenet
netman	manager, man, mgr, netmgr
network_mgt	netmgt
network_server	server
prime	primos, system
primenet	net, netlink
primos	prime, system
primos_cs	primos, prime, system
regist	
rje	
spool	

spoolbin	spool
syscol	
sysovl	
system	prime, primos, sys1, operator
system_debug	
system_manager	
tcpip_manager	
tele	
test	
timer_progress	
tools	

TOPS-10/20- An older and somewhat rare operating system, TOPS-10 ran on the DEC-10/20 machines. You can usually recognize a TOPS-10 by its' prompt, a lone period '.', while a TOPS-20 will have a '@' in its place. Most systems allow you to enter the commands 'SYSTAT' or 'FINGER' from the login prompt, before logging in. This command will let you see the users online, a valuable aide in hacking.
To login, type 'login xxx,yyy', where the x and y's are digits.
TOPS-10 does let you know when your username is incorrect.

COMMON ACCOUNTS

User ID Code	Password
1,2	OPERATOR, MANAGER, ADMIN, SYSLIB, LIB
2,7	MAINT, MAINTAIN, SYSMAINT
5,30	GAMES

IRIS- Unfortunely, i have no experience with IRIS whatsoever. To this day i haven't even seen one. So with regret i must present old material, the following info comes entirely from the LOD/H Technical Journal #3. Hopefully it will still be applicable.
The IRIS Operating System used to run soley on PDP systems, but now runs on many various machines.
IRIS will commonly present itself with a herald such as;
"Welcome to IRIS R9.1.4 timesharing"
And then an "ACCOUNT ID?" prompt.
IRIS is kind enough to tell you when you enter an incorrect ID, it won't kick you off after too many attempts, and no logs are kept. And strangely enough, passwords are not used!
So if you can find yourself an IRIS OS, try the following defaults and you should drop in..

COMMON ACCOUNTS

Username
accounting
boss
demo
manager
noname
pdp8
pdp11
software
tcl

NOS- The NOS(Network Operating System) is found on Cyber mainframes made by CDC(the Control Data Corporation).
Cyber machines are commonly run by institutions such as

universities and atomic research facilities.
Cybers will usually give a herald of some sort, such as
   Sheridan Park Cyber 180-830 Computer System
                or
   Sacremento Cyber 180-830 CSUS NOS Software System
The first login prompt will be 'FAMILY:', just hit <CR>.
The next prompt is 'USER NAME:'. This is more difficult, usually 7 characters. The password is even worse, commonly 7 random letters. Sound bad? It is. Brute forcing an account is next to impossible.
I've never seen these defaults work, but they are better than nothing. I got them out of the LOD/H Novice's Guide to Hacking, written by the Mentor. There are no known passwords for these usernames.

COMMON ACCOUNTS

Username

$SYSTEM
SYSTEMV

DECSERVER- The Decserver, is as the name implies, a server made by the Digital Equipment Corporation, the same company that makes the VAX machines.
It is possible the owner of the server put a password on it, if this is the case you will hit a # prompt. If the server has PADs or outdials on it, you can bet this is the case. You don't need a username, just the password. You will commonly get 3 tries, but it can be modified.
The default password is 'access', but other good things to try are ; server, dec, network, net, system (and whatever else goes along with that).
If you get past the #, or there isn't one, you will hit the prompt 'Enter Username>'. What you put really doesn't matter, it is just an identifier. Put something normal sounding, and not your hacker alias. It is actually interesting to look at the users online at a Decserver, as commonly there will be a few users
with the username C or CCC or the like, usually meaning they are probably a fellow hacker.
Also, at the Enter Username> prompt you are able to ask for help with the 'help' command, which spews out fairly lengthly logon help file.
If all went well you should end up at a 'Local>' prompt. Decservers have a fairly nice set of help files, simply type 'help' and read all you want.
It is a good idea to do a 'show users' when you first logon, and next do a 'show services' and 'show nodes'. The services are computers hooked up to the Decserver, which you can access. For obvious reasons you will often find many VAX/VMS systems on Decservers, but pretty much anything can be found Look for services titled Dial, Modem, PAD, X25, Network, or anthing like that. Try pretty much everything you see. Remember to try the usernames you see when you do a 'show users' as users for the systems online.
Also, you will sometimes find your Decserver has Internet (Telnet, SLIP or FTP) access, make sure you make full use of this.
To connect to the services you see, use 'c XXXX', where the X's represent the service name.
Once inside, the manufacturer's default for privs is 'system' and it is rarely changed.
The maintenance password changes from version to version.

With the Decserver 200 & 500 it is 0000000000000000 (16 0's), but with 300 it is simply 0.

GS/1- GS/1's are another server type system, but they are less common than the Decservers. The default prompt is 'GS/1>', but this can be changed to the sysadmins liking.
To check for a GS/1, do a 'sh d', which will print out some statistics.
To find what systems are available from the server, type 'sh n' or a 'sh c', and a 'sh m' for the system macros.

XMUX- The XMUX is a multiplexing system that provides remote access, made by Gandalf Technologies, Inc., Gandalf of Canada Ltd. in Canada. As far as I can tell, the XMUX is used only on Packet-Switched Networks, Datapac in particular but with usage on PSNs world wide.
The XMUX is not usually thought of as a stand alone system, but as a supportive system for multi-user networked systems, having a bit to do with system monitoring, channel control, and some of the features of multiplexing.
Thus, you'll commonly find a XMUX on a mnemonic or a subaddress of another system, although you will find them alone on their own NUA frequently as well.
To find the systems on a subaddress or a mnemonic, your best bet is to go with mnemonics, as the LOGGER mnemonic cannot be removed, while subaddressing is optional.
You won't always want to check every single system, so i'll give a guideline of where to check;
(REMINDER: this is only for systems on PSNs, and may not apply to your PSN)

- PACX/ Starmaster Systems : The PACX/Starmaster is also made by Gandalf, and the two are tightly interwoven. If mnemonics don't work, be sure to try LCNs, as the CONSOLE on a PACX/Starmaster is an entirely different thing, and frequently using the mnemonic CONSOLE will bring you to the PACX console, not the XMUX console.
- BBS Systems : BBS Systems on PSNs frequently need some help, and XMUXs are fairly commonly found with them.
- Other misc. systems : Many of the other operating systems, such as Unix, AOS/VS, Pick and HP3000 have the occasional XMUX along with it.
- Networked systems : A good portion of networked systems have XMUXs.

If a system does have a XMUX also, you can reach it almost always by the mnemonic CONSOLE, and if not, the node name of the XMUX. If that doesn't work, try LCNs up to and including 15.
Occasionally the console of the XMUX will be unpassworded, in which case you will drop straight into the console. The XMUX console is self-explanatory and menued, so i will leave you to explore it.
However, in all likeliness you will find yourself at the password prompt, 'Password >'. This can not be modified, but a one-line herald may be put above it.
To check for a XMUX, simply hit <CR>. It will tell you that the password was invalid, and it must be 1 to 8 alphanumeric characters.
As you can see, you do not need a username for the remote console of a XMUX. UIDs are used, but internally within the

workstation.
As it says, the password format is 1 to 8 alphanumeric characters. There is no default password, the console is left unprotected unless the owner decides to password it.
However, there are common passwords. They are;
console, gandalf, xmux, system, password, sys, mux xmux1
I'll repeat them in the common passwords again later.
But these will not always work, as it is up to the owner to pick the password(although they do like those).
Your next best bet is to find out the node name of the XMUX (XMUXs are polling systems as well, usually hooked up somehow to one of the regional hubs).
To do this, you must understand the parts of the XMUX.
The XMUX has 4 default parts; the CONSOLE, the FOX, the LOGGER, and the MACHINE.
I'll try and define the usage of them a bit more;

CONSOLE- the main remote part of the XMUX, which performs all the maintenance functions and system maintenance.
the actual system.
reachable usually on the LCN(subaddress) of 0 or 4/5, and the default mnemonic CONSOLE, which can be changed.

FOX - a test system, which runs through never ending lines of the alphabet and digits 0-9.
reachable on the LCN of 1, mnemonic FOX.

LOGGER - a device which displays log information, usually one or two lines, including the node name.
reachable on the LCN of 2, mnemonic LOGGER.

MACHINE- a system which i do not yet understand fully.
performs some interesting functions.
the prompt is '#'.
type 'S' and you will(always) receive a short/long (depending on how much the system is used) system status report, containing among other things the system node name.
if active, typing 'L' will bring up a more complete system log. This is VERY useful. It contains the NUAs of the systems which called the XMUX, and it contains the UIDs if used.

As you can see, the XMUX is rather complicated upon first look, but it is actually fairly simple. The easiest way to grab the node name is to call the LOGGER.
The logger MUST be present, always. It is a non-removable default. The LCN may be removed, but the mnemonic must stay.
I explained mnemonics earlier, but i'll refresh your memory.
To use the mnemonic, simply type the NUA, followed by a comma and then the mnemonic, ie;

12300456,LOGGER

The very first thing in the data string you see is the node name. If it is a blank space, you have run across a rarity, a XMUX without a node name.
The node name is THE most popular thing other than the other common passwords.
Try combinations of it, and combinations of it along with the words XMUX and MUX.
And of course, if a herald is used, use whatever you can find in the herald.
But again, if it is a company, they love to use the company name or acronym as a password, and that acronym or name will often be the node name.
Ok, have fun..

COMMON ACCOUNTS

Console Passwords

CONSOLE
XMUX
GANDALF
SYSTEM
PASSWORD
MUX
XMUX1
SYS
(node name)

One other thing. I did not include the profile or remote profile names, or the UIDs, as they are as far as i know inapplicable from remote.
And a final comment. XMUXs are powerful and potentially extremely harmful to a network. DO NOT DELETE ANYTHING. The only submenus you will have reason to access are 'DEFINE' and 'DISPLAY'. Don't boot people off channels or add console passwording or remove profiles..you will end up with your ass in jail. Taking down a network is less than funny to the people that run it. Explore, don't harm.

STARMASTER-/PACX

The Starmaster/PACX 2000 is still a somewhat mysterious system, but i have now explored all the security barriers as well as the network and the internal functions, so i feel this is fairly complete.
The Starmaster/PACX system is a networking/server system made by, again, Gandalf Technologies Inc., Gandalf of Canada Ltd., in Canada, and is also known informally (and some what incorrectly) as the 'Gandalf Access Server.' The Access is similar, but different, as described later.
It is a fairly popular system on Datapac, and has some usage in other regions of the world. Again, it is used mainly on Packet-Switched Networks, although, thanks to the dialing directory of a Sam24V outdial on a Starmaster, I have discovered that Starmasters do indeed have dialin access.
The first possible security barrier is the dialin password, which is rarely used, but you should know about.
The prompt is usually ;
   DIALIN PASSWORD?
But can be changed, although it should remain similar.
Dialin passwords are 1 to 8 characters, and are usually one of the following defaults;
   GANDALF SERVER PACX NET NETWORK STARMAST DIALIN PASSWORD
   ACCESS
If the Starmaster has a XMUX resident(explained in previous system definition; XMUXs), find out the node name and try it.
The next possible security barrier is that the sysadmin desires the users to enter a username/password before entering the server.
You will find yourself at a prompt such as;
   USERNAME?
This is the most common prompt.
Usernames are 1 to 8 characters, and the Starmaster will let you know if it is wrong or not with an error message such as;
   INCORRECT USERNAME
        or
   INVALID RESPONSE
This, like the username prompt, can be changed, but it will usually be in all-caps.
You are allowed between 1 and 10 attempts at either a valid username or a valid password, depending on the owners preference.

This means(if it is set to ten tries) you can enter 9 invalid usernames, and on the tenth enter a valid username, then have 10 attempts at a valid password.
The defaults for this(which i will list later also) prompt are; TEST, TESTUSER, TESTER, GANDALF, SYSTEM, GUEST
USER, HP, CONSOLE, and finally OPERATOR.
Also, first names will work usually.
The next prompt you will face, or the first one if usernames are not implemented, is the server prompt. This is the main user prompt for a Starmaster, all major user commands are used from here.
But as you can guess, commands aren't used really, it is service names you desire.
Sometimes you will get a list upon entering the server, but other times you will just hit the server prompt, which usually looks something like;

```
     SERVICE?
        or
      CLASS?
        or even
      service?
        or
      class?
        or
      service
```

Or whatever the sysadmin feels like. 'SERVICE?' is the default, and the most common.
Keep in mind that the services CAN be passworded, but rarely are. In the case of passwording, use your imagination.
Another thing; from the PACX console, where the services are defined, there is an option which decides whether the service is allowed for remote users. If this is set to NO, then you are out of luck, you have to be in the workstation to use the command. This is common for the CONSOLE and the MAIL, and occasionally modems and PADs. You will get an error message something like 'SERVICE NOT ALLOWED'.
I will give a more complete list of common services, but I will list the defaults and the major ones now.

PAD, X25, X28- (or name of your PSN)		Will commonly take you to a Gandalf PAD, for which the default prompt is '*'. 'HELP' will bring up a list of commands.
MAIL	-	A non-removable default, but i've never seen it with the remote access flag in the ON position.
CONNECT	-	Another non-removable default which i have never seen with the remote access flag in the on position.
MODEM, DIAL	-	And variations therof. The common outdial is the Gandalf made Sam24V, which comes with a great set of help files.
CONSOLE	-	The motherlode. The system controller, maintenance computer, test machine, and all of that. DON'T confuse the PACX console with the XMUX console, they are two very different things. The console should be protected by the sysadmin with his/her life, as every faction of the Starmaster is controlled from within the Console. The CONSOLE is a non-removable service from the server, BUT remote access can be removed thus cutting off our means of getting to it. Try it first, if it works the screen will

scroll down a number of lines and give this herald/prompt;

GANDALF TECHNOLOGIES INCORPORATED, COPYRIGHT 1990

OPERATOR NAME?

This is not changable, it will remain the same except for possibly the copyright date. There can be 8 operators at the most, and they will have 1 to 8 characters in their name and password. And again, the PACX will tell you if your operator name is incorrect. You will be allowed 1 to 10 attempts at the login name and then it resets to 0 for the password attempt when you've found an operator name, but same limit.

The same defaults for the usernames work here, if you are lucky, with the exception of HP. I'll list them again at the end.

Once you get in, it is all menued and explanatory. DON'T FUCK THINGS UP. By that I mean deleting or modifying. Look. There is MUCH to see. The PACX console is incredibly powerful, and you will have much more fun exploring it.

Besides, once you are in the console, the game is over. You have control over all the services, users, and all security barriers. If you get a high level console account, you are the God of the PACX, no joke.

COMMON ACCOUNTS

Usernames	Passwords
CONSOLE	CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM
GAND	GAND
GANDALF	GANDALF, SYSTEM, PACX, STARMAST, SYS
GUEST	GUEST, VISITOR, USER
HP	HP
OPERATOR	OPERATOR, SYSTEM, SYSLIB, LIB, GANDALF
SYSTEM	SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF
TEST	TEST, TESTUSER, USER, TESTER
TESTUSER	TEST, TESTUSER, USER, TESTER
TESTER	TEST, TESTUSER, USER, TESTER
USER	USER, GUEST, TEST, VISITOR, GANDALF

(i've never seen an account such as MAINT, but i would guess one exists, along with standard system defaults. Try anything outside these lines)

Services

1 (if it works; higher)
A (through Z)
10 (if it works; higher in sequence of tens)
BBS
CLUSTER
CONNECT
CONSOLE
DATABASE
DATAPAC
DEC
DIAL
DIALOUT
FILES
FTP

GATEWAY
GEAC
HELP
HP
INTERNET
LIB
LIBRARY
LOOP
MAIL
MENU
MODEM
MUX
NET
NETWORK
OUT
OUTDIAL
PACX12
PACX24
PACX96
PAD
PRIME
PRIMOS
PROD
SALES
SERVER
SUN
SUNOS
SYS
SYSTEM
TELNET
TYMNET
UNIX
VAX
VMS
X25
X28
XCON
XGATE
XMUX

And anything else you can think of.
First names are also fairly common.

Operator Name	Password
TEST	TEST, TESTUSER, USER, TESTER
TESTUSER	TEST, TESTUSER, USER, TESTER
TESTER	TEST, TESTUSER, USER, TESTER
GANDALF	GANDALF, SYSTEM, PACX, CONSOLE, SYS
GUEST	GUEST, VISITOR, USER
SYSTEM	SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF CONSOLE
USER	USER, GUEST, TEST, VISITOR, GANDALF
OPERATOR	OPERATOR, SYSTEM, CONSOLE, GANDALF
CONSOLE	CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM
SYS	SYS, SYSTEM, GANDALF, PACX, CONSOLE

And again, try first names and ANYTHING you can think of.
Getting into the console should be your main objective.

ACCESS2590- The Access2590 is another Gandalf creation. While it is a server system, it is different in some respects to a PACX. The Starmaster generally only connects computers on a local

or wide area network(they do connect to X.25 & IP addresses, but they *usually* don't), while the Access 2590 connects to local & wide area network services, X.25 address, and IP addresses with suprising versatility. The PACX is, however, in much wider distribution.
It will usually have an initial herald screen, often letting you know that it is indeed an Access server made by Gandalf. If the operator wishes he can include a menu of services with their respective descriptions in this provided space. Then you will find yourself at a prompt, the default being "Access 2590 >". I haven't seen any sort of initial protection before you hit that prompt, but i'm betting it does exist, and it probably goes along the lines of the PACX. Follow the trend I set with the PACX and you should do fine.
Anyways, the one thing I like so much more about the Access 2590 compared to the Starmaster is the command "show symbols" . That was one of the big problems from a hacking point of view with the PACX; it doesn't have a command available to show you the services. If you get console access on the PACX you can get a listing of services that way, but you simply cannot hack a console account everytime, and besides that often the owner will have turned the remote console access flag off.
If the operator wanted to give you help with services he had to take the initiative himself and design a herald screen or implement a help service, and few do. But the "show symbols" on an Access will give you a listing of all the available "symbols", which is Gandalf's term for services. Connect to them with "c xxx" where "xxx" is of course the service.
And yes, to you eager folks who have tasted the PACX console's power, the Access does have a console. Type "c console" to get to it.
Follow the PACX's guidelines, and you'll do fine.

PICK-

The PICK system was created by Dick Pick(no joke), and is a fairly widespread system, there are a few of them out there on the major PSNs. I really dislike PICK, but for those of you wishing to try it yourself, it is a fairly easy hack.
A normal PICK login prompt looks somewhat like;

```
     07 JUN 1993 04:00:21 Logon please:
```

Additional data can be entered in that line, and a header may be used above that. However, PICKs are usually recognizable by that logon prompt which will normally contain the date and time, as well as the 'Logon please:'.
If you aren't sure, enter the username 'SYSPROG', in ALL CAPS , as PICK is case sensitive and SYSPROG will be in capitals.
SYSPROG is the superuser(or as PICK calls it the 'Ultimate User') and is similar to root on a Unix; it must be present.
PICK lets you know when you've entered an invalid Username, which is helpful when finding valid accounts.
Experiment with the upper and lower case if you wish, but upper case is the norm.
The people who make PICK like to think of PICK as more a DBMS than an OS, and it is often sold just as that. Because of that, you may find it on Unix, MPE, and Primos based systems among others.
One last note, internal passwording is possible on the PICK, so don't be too suprised if you think you've found an unpassworded system only to be hit by a password before the internal prompt.

COMMON ACCOUNTS

Usernames	Passwords

---	---
1	
ACC	
ACCT	
ACCTNAME	
ACCUMATH	
ACCUPLOT	
ACCUPLOT-DEMO	ACCUPLOT, DEMO
ARCHIVE	
AUDITOR	
AUDITORS	
BACKUP	
BATCH	
BLOCK-CONVERT	
BLOCK-PRINT	
COLDSTART	
COMBINATION	
COMM	
COMTEST	
CPA	
CPA.DOC	CPA, DOC
CPA.PROD	CPA, PROD
CTRL.GROUP	CTRL, CONTROL
DEMO	
DA	
DCG	
DEV	
DM	DATA, MANAGER, MAN, MGR, DATAMGR, DATAMAN
DOS	
ERRMSG	
EXCEPTIONAL	
EXECUTE-CONTROL	
EXPRESS.BATCH	EXPRESS, BATCH
FILE-SAVE	FILESAVE, SAVE
FILE-TRANSFER	
FINANCE	
FLUSHER	
FMS	
FMS.PROD	FMS, PROD
GAMES	
GAMES.DOS	GAMES
GENERAL	
INSTANT	
INSTANT.DOS	INSTANT
JOB	
KILL	
LEARN	
LEARN.DLR	LEARN, DLR, LEARNDLR
LOGON	
LOTUS	
LOTUS.DOS	LOTUS
MAIL.BOX	MAIL
MINDER	
MODEM-SECURITY	
MOTD.DATA	MOTD
NETCOM	
NET.OFF	
NETOFF	
NETUSER	
NETWORK	
NEWAC	
NOLOG	
OLD.USER	
ON-LINE-DIAGS	DIAGS

```
PERFECT-BKGRND
POINTER-FILE
PRICE.DOS          PRICE
PRICES.DOS         PRICES
PROCLIB            PROC, LIBRARY, LIB
PROD
PROMCOR
PROMIS-ARCHIVE     PROMIS, ARCHIVE
PROMIS-BKGRND      PROMIS, BKGRND
PROMO
PWP
QA                 QUALITY, CONTROL
SCC.SYSPROG        SCC, SYSPROG
SCREENLIB
SECURITY
SET.PLF            SET, PLF, PLFSET
SL
SPSYM
STUDENT
SUPPORT
SYM.DOS            SYM
SYS
SYS.DOC            SYS
SYSLIB             SYSTEM, LIBRARY, SYS, LIB
SYSPROG            SYSTEM, PROGRAM, SYS, PROG, OPERATOR, DM
SYSPROG-PL         SYSPROG, PL
SYSTEM-ERRORS
TCL
TEMP
TEMP-SYSPROG       TEMP, SYSPROG
TEST
TEST-BKGRND        TEST
TRAINING
TRY.DOS            TRY
ULTICALC
ULTILINK
ULTIMATION
UNIMAX
WORDS
WP
WP.DOS             WP
WP42.DOS           WP, WP42
WP50.DOS           WP, WP50
WP51               WP, WP51
WP51.DOS           WP, WP51
XES
```

AOS/VS- AOS/VS is made by Data General Corporation(DGC), and is in my opinion the worst operating system i've seen yet.
But, in the quest of knowledge, and to broaden your computer horizons, i suggest that you try to hack even this system, for what it's worth.
The AOS/VS will usually readily identify itself with a banner such as;
(yes, i'm overstepping my margin, i apologize)

```
**** AOS/VS Rev 7.62.00.00 / Press NEW-LINE to begin logging on ****

AOS/VS 7.62.00.00 / EXEC-32 7.62.00.00  11-Jun-93  0:27:31      @VCON1

          Username:
```

The username prompt looks deceivingly like a VMS, but it is not, and you can be sure by entering garbage for the username

and password. The AOS/VS will reply;

```
      Invalid username - password pair
```

AOS/VS will not let you know when you've entered an incorrect username.
And a standard system will let you have 5 tries at a username/ password combination, but after that it gives this annoying message;

```
    Too many attempts, console locking for 10 seconds
```

Having the system lock for 10 seconds does really nothing to the hacker, except slow brute forcing down a small bit(10 seconds).
Anyways, once inside 'HELP' will give you a set of help files which i didn't enjoy too much, and 'WHO' will list the users online.

COMMON ACCOUNTS

Username	Password
guest	
op	operator, op
sysmgt	sys, mgt, system, man, mgr, manager
test	
user	

RSTS- Probably the oldest OS that is still out there is RSTS. RSTS was a very common OS a decade or so ago, but is now nearing extinction. However, there are still a few out there on PSNs, and thus you might want to attempt to hack in.
The RSTS will usually identify itself like;

```
    RSTS V9.7-08    93.06.10    02:36
    User:
```

Before attempting to hack, try the SYSTAT command. It is likely it will be disabled, but it is worth a try.
RSTS will tell you if the ID you've entered is incorrect with the error message;

```
    ?Invalid entry - try again
```

The UIDs are in the format xxx,yyy , where x and y are digits. Just guess at UIDs until you hit one with a password.
Also, the IDs will generally not go above 255 in both the x and y spots(ie: 255,255 is generally the highest ID).

COMMON ACCOUNTS

User ID	Password
1,2	SYSLIB

WNT- I really don't know much about Windows NT, mostly having to do with the fact that it was just released a little while ago and I have not seen it in action to this date. I don't know at what time in the future it will become widespread, but for you future hackers I did a little research and came up with the two manufacturer defaults; administrator and guest. Both come unpassworded.. administrator is the equivalent to root on a Unix, and guest is just as you'd expect .. a low level guest account. Interestingly enough, in the manuals I saw WNT sysadmins were encouraged to keep the guest account... unpassworded at that! Highly amusing.. let's see how long that lasts! Anyways..
Oh yeah.. case sensitive, too.. I'm pretty sure it is lowercase, but it is possible that the first letter is capitalized. Remember that when attempting to brute force new accounts. Oh, and keep in mind possible accounts such as

"test" and "field" and the such.

COMMON ACCOUNTS

Username
administrator
guest

NETWARE- Novell Netware is the most common PC LAN software and is a popular among high-schools. The internal (and external for that matter) security is poor.

COMMON ACCOUNTS

Username	Password
admin	operator, supervisor, sysadm
backup	
guest	visitor, user
netware	
novell	netware
public	
remote	
server	
staff	
supervisor	admin, operator, sysadm, supervis, manager
system1	
tape	backup
test	testuser
user	
visitor	guest

Sys75/85- AT&T's System75/85 have made a big splash in recent months despite their being around for years previous.. mostly due to codez kids discovering the PBX functions.
Anyways, the hype has pretty much died down so it is probably safe to post the defaults. If you don't like my doing this, suck yourself. Anyone with access to this file probably has them by now anyways. And if not, all the better. Free information has always been one of our primary goals, and I don't intend to change that for some insecure pseudo-hackers.

COMMON ACCOUNTS

Username	Password
browse	looker
craft	crftpw, craftpw
cust	custpw
field	support
inads	indspw, inadspw
init	initpw
rcust	rcustpw

AS400- Another OS that was only really in use before my time, AS-400 is IBM made. I pulled this from the old UPT messages, thanks to anybody who contributed.
It should in fact identify itself as an AS-400 at login time. I'm unsure of the case-sensativity of the characters.. i'll enter them as lowercase, but if unsuccessful use caps.

COMMON ACCOUNTS

Username
qsecofr
qsysopr
quser
sedacm
sysopr
user

TSO- An IBM product, TSO can be found stand alone, but is commonly found off an ISM.
Upon connect you should see a login prompt that looks like:

```
    IKJ56700A   ENTER USERID-
```

Or something close.
It will tell you if the username entered is incorrect:

```
    IKJ56420I   USERID xxx NOT AUTHORIZED TO USE TSO
    IKJ56429A   REENTER-
```

Occasionally some of the accounts will have the STC attribute and can not be used for remote login.

COMMON ACCOUNTS

Username	Password
admin	adm, sysadm, op
guest	
init	
maint	
systest	test
test1	test
tso	

BRUTE FORCE

Passwords

Occasionally you will find yourself in a position where you wish to penetrate a system, but defaults are taken off and social engineering is not possible.

The dedicated hacker then begins the tedious process of trying password after password, hoping to crowbar his way into the system. Thus the term 'Brute Force' was born, aptly describing this process.

Brute force is the absolute ugliest way of obtaining an account, but is is often effective. It is ugly for a number of reasons, having to do with the fact that you will have to call the system hundreds of times if the account is not easily brute forced.

However, first i will explain a modified form of brute force; intelligent brute force. In this process, the hacker tries the users first name, as that is the most common password of all, and a database of 20-100 common passwords.

The difference between this and the normal brute forcing is you cut your time down considerably, but your chances of getting in go down as well.

Normal brute forcing is rarely done nowadays; the greats of yesterday would spend 6 hours at a sitting trying passwords, but people nowadays seem to think 5 minutes is sufficient. Ugh.

If standard brute forcing is done, it is accomplished with automation, usually. Meaning the hacker will set up a program or a script file to spew out dictionary passwords for him, then go to the movies or whatever. Obviously, any way you do it, standard brute forcing is fairly dangerous. A sysadmin is more likely to notice you trying a username/password 2000 times than 50. If

you choose to do automated brute forcing, it might be a good idea to set up a hacked system to do it for you, such as a procured Unix. I would not, however, suggest wasting the powers of a Cray on such a menial task as brute force. You can only go as fast as the host system will let you. The danger in this is obvious, you will have to be connected to the remote system for a long time, leaving you wide open for a trace. It is up to you.

And, of course, brute forcing requires a username. If you don't have a username, you are probably out of luck.

One thing you should definetly do is make a list of first names, and make it fairly complete. Buy/steal a baby names book or look inside your phone book and copy down the more commmon names on to a piece of paper or into a file. Other than first names, husband/wife, boyfriend/girlfriend and childs names are the most common passwords.

Ok, here are the basics to intelligent brute force hacking;

1. try the users first name
2. try your list of first names, male and female
2. try the users first name, with a lone digit(1 to 9) after the username
3. try the users first name, with a lone digit(1 to 9) after the username
4. try the users first name, with a letter appended to the end(A to Z)
5. try anything related to the system you are on. If you are on a VAX running VMS on the Datapac PSN, try VAX, VMS, Datapac, X25, etc
6. try anything related to the company/service the system is owned by. if the user is on a system owned by the Pepsi Cola company, try Pepsi, Cola, Pepsico, etc.
7. finally, try passwords from your list of common passwords. your list of common passwords should not be above 200 words.
   The most popular passwords are;

   password secret money sex smoke beer x25 system
   hello cpu aaa abc fuck shit

   Add on popular passwords to that as you see fit.
   Remember; most passwords are picked spontaneously, on whatever enters the users mind at that time(you know the feeling, i bet). Attempt to get into the users mind and environment, to think what he would think. If you can't do that, just try whatever comes to your mind, you'll get the hang of it.

Brute Forcing User Names

A different form of brute force is that when you need a username to hack passwords from. In order to guess a valid username, you must be on a system that informs you when your username is invalid; thus VMS and Unix are out of the question.

There are two types of usernames(by my definition); user and system.

The user usernames are the standard user's usernames. Examples would be John, Smith, JMS, JSmith, and JohnS.

The system usernames are special usernames used by the system operators to perform various functions, such as maintenance and testing. Since these usernames are not owned by actual people(usually), they are given a name which corresponds to their function.

Guessing either type is usually fairly easy.

User usernames are standardly in one of 2 formats; first name or last name the more common format being first name. Less common formats are initials, first initial/last name, and first name/last initial. Occasionally the username formats will have nothing to do with names at all, and will instead be 6 or 8 digit numbers. Have fun.

The users of a system will almost always have the same format as each other. When you guess one, guessing more shouldn't be too hard.

For first names, again consult the list you made from the baby names book.

For last names, construct a list of the most common last names, ideally out of the phone book, but if you are too lazy your mind will do fine. SMITH and JONES are the most common non-foreign names.

For initials, use common sense. Guess at 3 letter combinations, and use sensible formats. Meaning don't use XYZ as a rule, go for JMS, PSJ, etc, to follow along with common first names and last names.

If you are getting no luck whatsoever, try switching your case(ie: from all lower case to all upper case), the system might be case sensitive.

Usually guessing system names shouldn't be necessary; I gave a default list for all the major systems. But if you run across a system not listed, you will want to discover defaults of your own. Use common sense, follow along with the name of the new OS and utilities that would fit with that name. Attempt to find out the username restrictions for that system, if usernames have to be 6 characters long, try only 6 character user names.
And finally, here is a list of common defaults(they are capitalized for convienience, but as a rule use lower case);

OPERATOR SYSOP OP OPER MANAGER SYSMAN SYSMGR MGR MAN ADMIN
SYSADMIN ADM SYSADM BOSS MAIL SYSTEM SYS SYS1 MAINT SYSMAINT
TEST TESTER TESTUSER USER USR REMOTE PUB PUBLIC GUEST VISITOR
STUDENT DEMO TOUR NEWS HELP MGT SYSMGT SYSPROG PROD SALES
MARKET LIB LIBRARY FILES FILEMAN NET NETWORK NETMAN NETMGR
RJE DOS GAMES INFO SETUP STARTUP CONTROL CONFIG DIAG SYSDIAG
STAT SYSDIAGS DIAGS BATCH SUPRVISR SYSLIB MONITOR UTILITY
UTILS OFFICE CORP SUPPORT SERVICE FIELD CUST SECURITY WORD
DATABASE BACKUP FRIEND DEFAULT FINANCE ACCOUNT HOST ANON
SYSTEST FAX INIT INADS SETUP

Brute Forcing Services

There is also the time when you are on a server system, and you need places to go. You will surely be told if the service you've entered is incorrect, so just try things that come to mind, and the following list; (the server may be case sensitive..use upper or lower case as you wish)
(NOTE: Try digits(1 +) and letters(A-Z) also)

SERVER NETWORK NET LINK LAN WAN MAN CONNECT LOG LOGIN HELP DIAL
OUT OUTDIAL DIALOUT MODEM MODEMOUT INTERNET TELNET PAD X25 X28 FTP
SYSTEM SYS SYS1 SYSTEM1 UNIX VAX VMS HP CONSOLE INFO CMDS LIST
SERVICES SERVICE SERVICE1 COMP COMPUTER CPU CHANNEL CHANNEL1 CH1
CH01 GO DO ? LOG ID USERS SHOW WHO PORT1 PORT NODE1 NODE LINK1
DISPLAY CONFIG CONTROL DIAGS SYSDIAGS DIAG SYSDIAG HELLO EMAIL
MAIL SET DEFINE PARAMS PRINT PHONE PHONES SESSION SESSION1 BEGIN
INIT CUST SERVICE SUPPORT BUSINESS ACCT ACCOUNT FINANCE SALES
BUFFER QUEUE STAT STATS SYSINFO SYSTAT FTP ACCESS DISK LIB SYSLIB
LIBRARY FILES BBS LOOP TEST SEARCH MACRO CALL COMMANDS TYPE FIND
ASK QUERY JOIN ATTACH JOB REMOTE COM1 COM CALLER LOGGER MACHINE
BULLITEN CLUSTER RUN HELLO PAYROLL DEC

SOCIAL ENGINEERING

While I am in no way going to go indepth on SE(social engineering) at this point, i will explain the premise of SE to those new to it.

Social engineering can be defined any number of ways, but my definition goes along the lines of; "Misrepresentation of oneself in a verbal manner to another person in order to obtain knowledge that is otherwise unattainable." Which in itself is a nice way of putting "manipulation, lying and general bullshitting".

Social engineering is almost always done over the phone.

I'll give an example. The hacker needs information, such as an account, which he cannot get by simple hacking. He calls up the company that owns the system he wishes to penetrate, and tells them he is Joe Blow of the Computer Fixing Company, and he is supposed to fix their computers, or test them remotely. But gosh, somebody screwed up and he doesn't have an account. Could the nice lady give him one so he can do his job and make everybody happy?

See the idea? Misrepresentation of the truth; pretending to be someone you

aren't.

If you are skeptical, you shouldn't be. SE is tried and true, due to the fact that any company's biggest security leak is their employees. A company can design a system with 20 passwords, but if an uncaring employee unwittingly supplies a hacker with all of these passwords, the game is over.

You *must* have the voice for it. If you sound like a 12 year old, you aren't going to get shit. If you can't help it, there are telephone-voice changers(which any SE practicer should have anyways) that will do it for you.

If the person wishes to contact higher authority(who will probably suspect somethings up), get mad. Don't go into a rage, but do get angry. Explain that you have a job to do, and be persuasive.

I won't go more into SE, there are tons of text files out there on it already. Just remember to keep calm, have a back up plan, and it is a good idea to have the script on paper, and practice it a bit before hand. If you sound natural and authorative, you will get whatever you want.

And practice makes perfect.

TRASHING

Trashing is another thing i will not go too indepth on, but i will provide a very quick overview.

Trashing is the name given to the process of stealing a companies trash, then rooting through it and saving the valuable information.

Trashing is practiced most often on the various RBOCs, but if you are attempting to hack a system local to you, it might be a good idea to go trashing for a few weeks, you might find a printout or a scrap of paper with a dialup or username and password written on it.

ACRONYMS

This is a basic list of H/P acronyms I've compiled from various sources.. it should be big enough to serve as an easy reference without being incredibly cumbersome

ABSBH:	Average Busy Season Busy Hour
AC:	Area code
ACC:	Automatic Communications Control
ACC:	Asynchronous Communications Center
ACD:	Automatic Call Distributor
ACE:	Automatic Calling Equipment
ACF:	Advanced Communications Functions
ACN:	Area Code + Number
ADPCM:	Adaptive Differential Pulse Code Modulation
AIS:	Automatic Intercept System
ALFE:	Analog Line Front End
ALRU:	Automatic Line Record Update
AM:	Account Manager
AM:	Access Module
AM:	Amplitude Modulation
AMA:	Automatic Message Accounting
AMSAT:	American Satellite
AN:	Associated Number
ANI:	Automatic Number Identification
ANXUR:	Analyzer for Networks with Extended Routing
AOSS:	Auxiliary Operator Services System
AP:	Attached Processor
ARC:	Automatic Response Control
ARP:	Address Resolution Protocol
ARPA:	Advanced Reasearch Projects Agency
ARS:	Automatic Response System

ARSB: Automated Repair Service Bureau
AT: Access Tandem
ATB: All Trunks Busy
ATH: Abbreviated Trouble History
ATM: Automated Teller Machine
ATM: Asynchronous Transfer Mode
AT&T: American Telegraph and Telephone Company
AVD: Alternate Voice Data
BCD: Binary Coded Decimal
BCUG: Bilateral CUG
BELLCORE: Bell Communications Research
BGP: Border Gateway Protocol
BHC: Busy Hour Calls
BLV: Busy Line Verification
BOC: Bell Operating Company
BOR: Basic Output Report
BOS: Business Office Supervisor
BSC: Binary Synchronous Module
BSCM: Bisynchronous Communications Module
BSOC: Bell Systems Operating Company
CA: Cable
CADV: Combined Alternate Data/Voice
CAMA: Centralized Automatic Message Accounting
CATLAS Centralized Automatic Trouble Locating & Analysis System
CAU: Controlled Access Unit
CAVD: Combined Alternated Voice/Data
CBC Cipher Block Chaining
CBS: Cross Bar Switching
CBX: Computerized Branch Exchange
CBX: Computerized Business Exchange
CC: Calling Card
CC: Common Control
CC: Central Control
CC: Country Code
CCC: Central Control Complex
CCC: Clear Channel Capability
CCC: Central Control Computer
CCIS: Common Channel Interoffice Signalling
CCITT: International Telephone and Telegraph Consultative Committee
CCM: Customer Control Management
CCNC: Common Channel Network Controller
CCNC: Computer Communications Network Center
CCS: Common Channel Signalling
CCSA: Common Control Switching Arrangement
CCSA: Common Central Switching Arrangement
CCSS: Common Channel Signalling System
CCT: Central Control Terminal
CCTAC: Computer Communications Trouble Analysis Center
CDA: Call Data Accumulator
CDA: Crash Dump Analyzer
CDA: Coin Detection and Announcement
CDAR: Customer Dialed Account Recording
CDC: Control Data Corporation
CDI: Circle Digit Identification
CDO: Community Dial Office
CDPR: Customer Dial Pulse Receiver
CDR: Call Dial Recording
CDS: Cicuit Design System
CEF: Cable Entrance Facility
CERT: Computer Emergency Response Team
CF: Coin First
CGN: Concentrator Group Number
CI: Cluster Interconnect
CIC: Carrier Identification Codes

CICS: Customer Information Control System
CID: Caller ID
CII: Call Identity Index
CIS: Customer Intercept Service
CISC: Complex Instruction Set Computing
CLASS: Custom Local Area Signalling Service
CLASS: Centralized Local Area Selective Signalling
CLDN: Calling Line Directory Number
CLEI: Common Language Equipment Identification
CLI: Calling Line Identification
CLID: Calling Line Identification
CLLI: Common Language Location Indentifier
CLNP: Connectionless Network Protocol
CMAC: Centralized Maintenance and Administration Center
CMC: Construction Maintenance Center
CMDF: Combined Main Distributing Frame
CMDS: Centralized Message Data System
CMIP: Common Management Information Protocol
CMS: Call Management System
CMS: Conversational Monitoring System
CMS: Circuit Maintenance System
CMS: Communications Management Subsystem
CN/A: Customer Name/Address
CNA: Communications Network Application
CNAB: Customer Name Address Bureau
CNCC: Customer Network Control Center
CNI: Common Network Interface
CNS: Complimentary Network Service
CO: Central Office
COC: Central Office Code
COCOT: Customer Owned Coin Operated Telephone
CODCF: Central Office Data Connecting Facility
COE: Central Office Equipment
COEES: Central Office Equipmet Engineering System
COER: Centarl Office Equipment Reports
COLT: Central Office Line Tester
COMSAT: Communications Satellite
COMSEC: Communications Security
COMSTAR: Common System for Technical Analysis & Reporting
CONS: Connection-Oriented Network Service
CONTAC: Central Office Network Access
COS: Class of Service
COSMIC: Common Systems Main Inter-Connection
COR: Class Of Restriction
COSMOS: Computerized System For Mainframe Operations
COT Central Office Terminal
CP: Control Program
CPBXI: Computer Private Branch Exchange Interface
CPC: Circuit Provisioning Center
CPD: Central Pulse Distributor
CPMP: Carrier Performance Measurement Plan
CRAS: Cable Repair Administrative System
CRC: Customer Record Center
CRC: Customer Return Center
CREG: Concentrated Range Extension & Gain
CRG: Central Resource Group
CRIS: Customer Record Information System
CRS: Centralized Results System
CRSAB: Centralized Repair Service Answering Bureau
CRT: Cathode Ray Tube
CRTC: Canadian Radio-Television and Telecommunications Commission
CSA: Carrier Servicing Area
CSAR: Centralized System for Analysis and Reporting
CSC: Cell Site Controller

CSC: Customer Support Center
CSDC: Circuit Switch Digital Capability
CSP: Coin Sent Paid
CSMA/CD: Carrier Sense Multiple Access/Collission Detection
CSR: Customer Service Records
CSS: Computer Special Systems
CSS: Computer Sub-System
CSU: Channel Service Unit
CT: Current Transformer
CTC: Channel Termination Charge
CTC: Central Test Center
CTM: Contac Trunk Module
CTMS: Carrier Transmission Measuring System
CTO: Call Transfer Outside
CTSS: Compatible Time Sharing System
CTSS: Cray Time Sharing System
CTTN: Cable Trunk Ticket Number
CTTY: Console TeleType
CU: Control Unit
CU: Customer Unit
CUG: Closed User Group
CWC: City-Wide Centrex
DA: Directory Assistance
DACC: Directort Assistance Call Completion
DAA: Digital Access Arrangements
DACS: Digital Access and Cross-connect System
DACS: Directory Assistance Charging System
DAIS: Distributed Automatic Intercept System
DAL: Dedicated Access Line
DAO: Directory Assistance Operator
DAP: Data Access Protocol
DARC: Division Alarm Recording Center
DARPA: Department of Defense Advanced Research Projects Agency
DARU: Distributed Automatic Response Unit
DAS: Device Access Software
DAS: Directory Assistance System
DAS: Distributor And Scanner
DAS: Dual Attachment Station
DASD: Direct Access Storage Device
DBA: Data Base Administrator
DBA: Digital Business Architecture
DBAC: Data Base Administration Center
DBAS: Data Base Administration System
DBC: Digital Business Center
DBM: Database Manager
DBMS: Data Base Management System
DBS: Duplex Bus Selector
DCA: Defense Communications Agency
DCC: Data Country Code
DCC: Data Collection Computer
DCE: Data Circuit-Terminating Equipment
DCE: Data Communicating Equipment
DCL: Digital Computer Language
DCLU: Digital Carrier Line Unit
DCM: Digital Carrier Module
DCMS: Distributed Call Measurement System
DCMU: Digital Concentrator Measurement Unit
DCO-CS: Digital Central Office-Carrier Switch
DCP: Duplex Central Processor
DCS: Digital Cross-Connect System
DCSS: Discontiguous Shared Segments
DCSS: Digital Customized Support Services
DCT: Digital Carrier Trunk
DDCMP: Digital Data Communications Message Protocol

DDD: Direct Distance Dialing
DDN: Defense Data Network
DDR: Datapac Design Request
DDS: Digital Data Service
DDS: Digital Data System
DDS: Dataphone Digital Service
DEC: Digital Equipment Corporation
DES: Data Encryption Standard
DF: Distributing Frame
DGC: Data General Corporation
DH: Distant Host
DID: Direct Inward Dialing
DIMA: Data Information Management Architecture
DINS: Digital Information Network Service
DIS: Datapac Information Service
DISA: Direct Inward System Access
DLC: Digital Loop Carrier
DLS: Dial Line Service
DM: Demultiplexer
DMA: Direct Memory Access
DN: Directory Numbers
DNA: Datapac Network Address
DNA: Digital Named Accounts
DNA: Digital Network Architecture
DNIC: Data Network Identifier Code
DNR: Dialed Number Recorder
DNS: Domain Name Service
DNS: Domain Name System
DOCS: Display Operator Console System
DOD: Department Of Defense
DOM: District Operations Manager
DPSA: Datapac Serving Areas
DPTX: Distributed Processing Terminal Executive
DSC: Data Stream Compatibility
DSI: Data Subscriber Interface
DSL: Digital Subscriber Line
DSN: Digital Services Network
DSU: Data Service Unit
DSU: Digital Service Unit
DSX: Digital Signal Cross-Connect
DTC: Digital Trunk Controller
DTE: Data Terminal Equipment
DTF: Dial Tone First
DTG: Direct Trunk Group
DTI: Digital Trunk Interface
DTIF: Digital Tabular Interchange Format
DTMF: Dual Tone Multi-Frequency
DTN: Digital Telephone Network
DTST: Dial Tone Speed Test
DVM: Data Voice Multiplexor
EAEO: Equal Access End Office
EA-MF: Equal Access-Multi Frequency
EBDI: Electronic Business Data Interchange
EC: Exchange Carrier
ECC: Enter Cable Change
EDC: Engineering Data Center
EDI: Electronic Data Interchange
EE: End to End Signaling
EEDP: Expanded Electronic Tandem Switching Dialing Plan
EGP: Exterior Gateway Protocol
EIES: Electronic Information Exchange System
EIU: Extended Interface Unit
EKTS: Electonic Key Telephone Service
ELDS: Exchange Line Data Service

EMA: Enterprise Management Architecture
EO: End Office
EOTT: End Office Toll Trunking
EREP: Environmental Recording Editing and Printing
ESA: Emergency Stand Alone
ESB: Emergency Service Bureau
ESN: Electronic Serial Number
ESP: Enhanced Service Providers
ESS: Electronic Switching System
ESVN: Executive Secure Voice Network
ETS: Electronic Tandem Switching
EWS: Early Warning System
FAC: Feature Access Code
FAM: File Access Manager
FCC: Federal Communications Commission
FCO: Field Change Order
FDDI: Fiber Distributed Data Interface
FDM: Frequency Division Multiplexing
FDP: Field Development Program
FEP: Front-End Processor
FEV: Far End Voice
FIFO: First In First Out
FIPS: Federal Information Procedure Standard
FM: Frequency Modulation
FMAP: Field Manufacturing Automated Process
FMIC: Field Manufacturing Information Center
FOA: First Office Application
FOIMS: Field Office Information Management System
FPB: Fast Packet Bus
FRL: Facilities Restriction Level
FRS: Flexible Route Selection
FRU: Field Replaceable Unit
FS: Field Service
FSK: Frequency Shift Keying
FT: Field Test
FTG: Final Trunk Group
FTP: File Transfer Protocol
FTPD: File Transfer Protocol Daemon
FX: Foreign Exchange
GAB: Group Access Bridging
GCS: Group Control System
GECOS: General Electric Comprehensive Operating System
GGP: Gateway-to-Gateway Protocol
GOD: Global Out Dial
GPS: Global Positioning System
GRINDER: Graphical Interactive Network Designer
GSA: General Services Administration
GSB: General Systems Business
GTE: General Telephone
HCDS: High Capacity Digital Service
HDLC: High Level Data Link Control
HLI: High-speed LAN Interconnect
HDSC: High-density Signal Carrier
HPO: High Performance Option
HUTG: High Usage Trunk Group
HZ: Hertz
IBM: International Business Machines
IBN: Integrated Business Network
IC: Intercity Carrier
IC: InterLATA Carrier
IC: Interexchange Carrier
ICAN: Individual Circuit Analysis Plan
ICH: International Call Handling
ICM: Integrated Call Management

ICMP: Internet Control Message Protocol
ICN: Interconnecting Network
ICPOT: Interexchange Carrier-Point of Termination
ICUG: International Closed User Group
ICVT: Incoming Verification Trunk
IDA: Integrated Digital Access
IDCI: Interim Defined Central Office Interface
IDDD: International Direct Distance Dialing
IDLC: Integrated Digital Loop Carrier
IDN: Integrated Digital Networks
IEC: Interexchange Carrier
IMP: Internet Message Processor
IMS: Information Management Systems
IMS: Integrated Management Systems
IMTS: Improved Mobile Telephone Service
INAP: Intelligent Network Access Point
INS: Information Network System
INTT: Incoming No Test Trunks
INWATS: Inward Wide Area Telecommunications Service
IOC: Interoffice Channel
IOC: Input/Output Controller
IOCC: International Overseas Completion Center
IP: Intermediate Point
IP: Internet Protocol
IPCF: Inter-Program Communication Facility
IPCH: Initial Paging Channel
IPCS: Interactive Problem Control System
IPL: Initial Program Load
IPLI: Internet Private Line Interface
IPLS: InterLATA Private Line Services
IPSS: International Packet-Switched Service
IRC: Internet Relay Chat
IRC: International Record Carrier
ISC: Inter-Nation Switching Center
ISDN: Integrated Services Digital Network
ISIS: Investigative Support Information System
ISO: International Standards Organization
ISSN: Integrated Special Services Network
ISU: Integrated Service Unit
ISWS: Internal Software Services
ITDM: Intelligent Time Division Multiplexer
ITI: Interactive Terminal Interface
ITS: Interactive Terminal Support
ITS: Incompatible Time-Sharing System
ITT: International Telephone and Telegraph
IVP: Installation Verification Program
IX: Interactive Executive
IXC: Interexchange Carrier
JCL: Job Control Language
JES: Job Entry System
KP: Key Pulse
LAC: Loop Assignment Office
LADS: Local Area Data Service
LADT: Local Area Data Transport
LAM: Lobe Access Module
LAN: Local Area Network
LAP: Link Access Protocol
LAPB: Link Access Protocol Balanced
LAPS: Link Access Procedure
LASS: Local Area Signalling Service
LASS: Local Area Switching Service
LAST: Local Area System Transport
LAT: Local Area Transport
LATA: Local Access Transport Area

LAVC: Local Area VAX Cluster
LBS: Load Balance System
LCDN: Last Call Directory Number
LCM: Line Concentrating Module
LCN: Logical Channel
LD: Long Distance
LDEV: Logical Device
LDM: Limited Distance Modem
LDS: Local Digital Switch
LEBC: Low End Business Center
LEC: Local Exchange Carrier
LEN: Low End Networks
LENCL: Line Equipment Number Class
LGC: Line Group Controller
LH: Local Host
LIFO: Last In First Out
LIP: Large Internet Protocol
LLC: Logical Link Control
LM: Line Module
LMOS: Loop Maintenance and Operations System
LSI: Large Scale Integration
LTC: Line Trunk Controller
LU: Local Use
LVM: Line Verification Module
MAC: Media Access Control
MAC: Message Authentication
MAN: Metropolitan Area Network
MAP: Maintenance and Administration Position
MAP: Manufacturing Automation Protocol
MAT: Multi-Access Trunk
MAU: Multistation Access Unit
MBU: Manufacturing Business Unit
MCA: Micro Channel Architecture
MCI: Microwave Communications, Inc.
MCP: Master Control Program
MCT: Manufacturing Cycle Time
MCU: Multi Chip Unit
MDR: Message Detail Record
MDS: Message Design Systems
MDU: Marker Decoder Unit
MF: Multi-Frequency
MFD: Main Distributing Frame
MFR: Mult-Frequency Receivers
MFT: Metallic Facility Terminal
MHZ: Mega-Hertz
MIB: Management Information Base
MIC: Management Information Center
MIF: Master Item File
MIS: Management Information Systems
MJU: MultiPoint Junction Unit
MLHG: Multiline Hunt Group
MLT: Mechanized Loop Testing
MNS: Message Network Basis
MOP: Maintenance Operation Protocol
MP: Multi-Processor
MPL: Multischedule Private Line
MPPD: Multi-Purpose Peripheral Device
MRAA: Meter Reading Access Arrangement
MSCP: Mass Storage Control Protocol
MSI: Medium Scale Integration
MTBF: Mean Time Between Failure
MTS: Message Telecommunication Service
MTS: Message Telephone Service
MTS: Message Transport Service

MTS: Mobile Telephone Service
MTSO: Mobile Telecommunications Switching Office
MTU: Maintenence Termination Unit
MUX: Multiplexer
MVS: Multiple Virutal Storage
MWI: Message Waiting Indicator
NAM: Number Assignment Module
NAS: Network Application Support
NC: Network Channel
NCCF: Network Communications Control Facility
NCI: Network Channel Interface
NCIC: National Crime Information Computer
NCP: Network Control Program
NCS: Network Computing System
NCTE: Network Channel Terminating Equipment
NDA: Network Delivery Access
NDC: Network Data Collection
NDIS: Network Device Interface Specification
NDNC: National Data Network Centre
NDS: Network Data System
NDU: Network Device Utility
NEBS: Network Equipment Building System
NECA: National Exchange Carriers Association
NFS: Network File Sharing
NFS: Network File System
NFT: Network File Transfer
NI: Network Interconnect
NI: Network Interface
NIC: Network Information Center
NIC: Network Interface Card
NJE: Network Job Entry
NLM: Netware Loadable Modules
NLM: Network Loadable Modules
NM: Network Module
NMR: Normal Mode Rejection
NOS: Network Operating System
NPA: Numbering Plan Area
NPA: Network Performance Analyzer
NSF: National Science Foundation
NSP: Network Services Protocol
NTE: Network Terminal Equipment
NUA: Network User Address
NUI: Network User Identifier
OC: Operator Centralization
OCC: Other Common Carrier
OD: Out Dial
ODA: Office Document Architecture
ODDB: Office Dependent Data Base
ODI: Open Data Interface
OGT: Out-Going Trunk
OGVT: Out-Going Verification Trunk
OIS: Office Information Systems
OLTP: On-Line Transaction Processing
ONI: Operator Number Identification
OPCR: Operator Actions Program
OPM: Outside Plant Module
OPM: Outage Performance Monitoring
OR: Originating Register
OS: Operating System
OSI: Open Systems Interconnection
OSL: Open System Location
OSS: Operator Services System
OST: Originating Station Treatment
OTC: Operating Telephone Company

OTR: Operational Trouble Report
OUTWATS: Outward Wide Area Telecommunications Service
PABX: Private Automated Branch Exchange
PACT: Prefix Access Code Translator
PAD: Packet Assembler/Disassembler
PADSX: Partially Automated Digital Signal Cross-Connect
PAM: Pulse Amplitude Modulation
PAX: Private Automatic Exchange
PBU: Product Business Unit
PBX: Private Branch Exchange
PC: Primary Center
PCM: Pulse Code Modulation
PCP: PC Pursuit
PFM: Pulse Frequency Modulation
PGA: Pin Grid Array
PIN: Personal Identification Number
PLA: Programmable Logic Array
PLD: Programmable Logic Device
PLS: Programmable Logic Sequencer
PM: Phase Modulation
PM: Peripheral Module
PMAC: Peripheral Module Access Controller
PMR: Poor Mans Routing
PNC: Primenet Node Controller
POC: Point of Contact
POF: Programmable Operator Facility
POP: Point of Presence
POS: Point Of Sale
POT: Point of Termination
POTS: Plain Old Telephone Service
PPN: Project Program Number
PPP: Point to Point Protocol
PPS: Public Packet Switching
PPSN: Public Packet Switched Network
PSAP: Public Safety Answering Point
PSDC: Public Switched Digital Capability
PSDCN: Packet-Switched Data Communication Network
PSDN: Packet-Switched Data Network
PSDS: Public Switched Digital Service
PSN: Packet-Switched Network
PSS: Packet-Switched Service
PSW: Program Status Word
PTE: Packet Transport Equipment
PTS: Position and Trunk Scanner
PTT: Postal Telephone & Telegraph
PVC: Permanent Virtual Call
PVN: Private Virtual Network
PWC: Primary Wiring Center
QPSK: Quadrature Phase-Shift Keying
RACF: Resource Access Control Facility
RAO: Revenue Accounting Office
RARP: Reverse Address Resolution Protocol
RBG: Realtime Business Group
RBOC: Regional Bell Operating Company
RC: Rate Center
RC: Regional Center
RDB: Relational Database
RDSN: Region Digital Switched Network
RDT: Restricted Data Transmissions
RDT: Remote Digital Terminal
REP: Reperatory Dialing
REXX: Restructured Extended Executer Language
RFC: Request For Comments
RIP: Routing Information Protocol

RIS: Remote Installation Service
RISC: Reduced Instruction Set Computer
RISD: Reference Information Systems Development
RJE: Remote Job Entry
RLCM: Remote Line Concentrating Module
RNOC: Regional Network Operations Center
ROTL: Remote Office Test Line
RPC: Remote Procedure Call
RPE: Remote Peripheral Equipment
RSA: Reference System Architecture
RSB: Repair Service Bureau
RSC: Remote Switching Center
RSCS: Remote Spooling Communications Subsystem
RSS: Remote Switching System
RSU: Remote Switching Unit
RTA: Remote Trunk Arrangement
RTG: Routing Generator
R/W: Read/Write
RX: Remote Exchange
SA: Storage Array
SABB: Storage Array Building Block
SAM: Secure Access Multiport
SARTS: Switched Access Remote Test System
SAS: Switched Access Services
SAS: Single Attachment System
SBB: System Building Block
SABM: Set Asynchronous Balanced Mode
SAC: Special Area Code
SBS: Satellite Business Systems
SC: Sectional Center
SCC: Specialized Common Carrier
SCC: Switching Control Center
SCCP: Signaling Connection Control Part
SCCS: Switching Control Center System
SCF: Selective Call Forwarding
SCF: Supervision Control Frequency
SCM: Station Class Mark
SCM: Subscriber Carrier Module
SCP: Signal Conversion Point
SCP: System Control Program
SCP: Service Control Point
SCR: Selective Call Rejection
SDLC: Synchronous Data Link Control
SF: Single-Frequency
SFE: Secure Front End
SIDH: System Identification Home
SIT: Special Information Tones
SLIC: Subscriber Line Interface Card
SLIM: Subscriber Line Interface Module
SLIP: Serial Line Internet Protocol
SLS: Storage Library System
SLU: Serial Line Unit
SM: System Manager
SMDI: Storage Module Disk Interconnect
SMDR: Station Manager Detail Recording
SMI: System Management Interrupt
SMP: Symmetrical Multi-Processing
SMS: Self-Maintenance Services
SMS: Station Management System
SMTP: Simple Mail Transfer Protocol
SNA: Systems Network Architecture
SNMP: Simple Network Management Protocol
SONDS: Small Office Network Data System
SOST: Special Operator Service Treatment

SP: Service Processor
SPC: Stored Program Control
SPCS: Stored Program Control System
SPCSS: Stored Program Control Switching System
SPM: Software Performance Montior
SQL/DS: Structured Query Language/Data System
SRC: System Resource Center
SS: Signaling System
SSAS: Station Signaling and Announcement System
SSCP: Systems Service Control Point
SSCP: Subsystem Services Control Point
SSP: Switching Service Points
SSS: Strowger Switching System
ST: Start
STC: Service Termination Charge
STD: Subscriber Trunk Dialing
STP: Signal Transfer Point
STS: Synchronous Transport Signal
SVC: Switched Virtual Call
SWG: Sub Working Group
SxS: Step-by-Step Switching
T-1: Terrestrial Digital Service
TAC: Trunk Access Code
TAC: Terminal Access Circuit
TAC: Terminal Access Center
TAS: Telephone Answering Service
TASI: Time Assignment Speech Interpolation
TBU: Terminals Business Unit
TC: Toll Center
TCAP: Transaction Capabilities ApplicationPart
TCC: Technical Consulting Center
TCC: Telecommunications Control Computer
TCF: Transparent Connect Facility
TCM: Time Compression Multiplexing
TCP: Transmission Control Protocol
TDAS: Traffic Data Administration System
TDCC: Transport Data Coordinating Committee
TDM: Time Division Multiplexer
TDMS: Terminal Data Management System
TDS: Terrestrial Digital Service
TH: Trouble History
TIDE: Traffic Information Distributor & Editor
TIS: Technical Information Systems
TLB: TransLAN Bridge
TM: Trunk Module
TMSCP: Tape Mass Storage Control Protocol
TNDS: Total Network Data System
TNPS: Traffic Network Planning Center
TO: Toll Office
TOP: Technical Office Protocol
TOPS: Traffic Operator Position System
TP: Transport Protocol
TP: Toll Point
TP: Transaction Processing
TPC: Transaction Processiong Performance Council
TREAT: Trouble Report Evaluation and Analysis Tool
TRIB: Throughput Rate in Information Bits
TRT: Tropical Radio and Telephone
TSB: Time Shared Basic Environment
TSG: Timing Signal Generator
TSN: Terminal Switching Network
TSO: Time Sharing Option
TSPS: Traffice Service Position System
TTL: Transistor-to-Transistor Logic

TTS: Trunk Time Switch
TWX: Type Writer Exchange
UA: Unnumbered Acknowledgement
UAE: Unrecoverable Application Error
UART: Universal Asynchronous Receiver Transmitter
UCS: Uniform Communication Standard
UDC: Universal Digital Channel
UDP: User Datagram Protocol
UDVM: Universal Data Voice Multiplexer
UID: User Identifier
UPC: Utility Port Conditioner
USC: Usage Surcharge
USDN: United States Digital Network
USTS: United States Transmission Systems
UUCP: Unix to Unix Copy Program
VAN: Value Added Networks
VAX: Virtual Address Extention
VCPI: Virtual Control Program Interface
VDU: Visual Display Unit
VF: Voice Frequency
VFU: Vertical Forms Unit
VFY: Verify
VIA: Vax Information Architecture
VLM: Virtual Loadable Module
VLSI: Very Large Scale Integration
VMB: Voice Mail Box
VMCF: Virtual Machine Communications Facility
VMS: Virtual Memory System
VMS: Voice Mail System
VM/SP: Virtual Machine/System Product
VPA: VAX Performance Advisor
VPS: Voice Processing System
VSAM: Virtual Storage Access Method
VSE: Virtual Storage Extended
VTAM: Virtual Telecommunications Access Method
VTOC: Volume Table Of Contents
VUIT: Visual User Interface Tool
VUP: Vax Unit of Processsing
WAN: Wide Area Network
WATS: Wide Area Telecommunications System
WATS: Wide Area Telephone Service
WC: Wiring Center
WCPC: Wire Center Planning Center
WDCS: Wideband Digital Cross-Connect System
WDM: Wavelength Division MultiPlexing
WES: Western Electronics Switching
WUI: Western Union International
XB: Crossbar Switching
XBAR: Crossbar Switching
XBT: Crossbar Tandem
XNS Xerox Network Systems
XSV Transfer Cost System Value
XTC Extended Test Controller

CONCLUSION

Last words

Well, i sincerely hope that this file was of some use to you, and i would encourage you to distribute it as far as you can. If you enjoyed it, hated it,

have suggestions, or whatever, feel free to email me at my Internet address(my only permanent one for now) or at a BBS, if you can find me.
    Have phun...

        - Deicide -

Recommended Reading

Neuromancer, Mona Lisa Overdrive, Count Zero and all the rest, by William Gibson
The Hacker Crackdown, by Bruce Sterling
Cyberpunk, by Katie Hafner and John Markoff
The Cuckoo's Egg, by Cliff Stoll
2600: The best h/p printed zine. $21 in American funds, U.S. & Canada.
      2600 Subscription Dept., P.O. Box 752, Middle Island NY 11953-0752
      Office: 516-751-2600   Fax: 516-751-2608
The issues of CUD, cDc, & Phrack electronic newsletters, and the LOD/H TJs, all of which can be found on the Internet and any good h/p oriented BBS.

BBSes

    Although most boards have a lifespan equivalent to that of a fruitfly, I finally have a list which is somewhat stable.. getting on them is your problem.. just be yourself and be willing to learn.

- Unphamiliar Territories
- Demon Roach Underground
- Temple of the Screaming Electron
- Burn This Flag
- Dark Side of the Moon

and Phrozen Realm if it returns..

References

    All the material used in this publication is original unless specifically stated otherwise.
    However, i'd like to thank Phrack and the LOD/H for their textfiles which gave me a valuable push in the right direction..
    And of course all the great h/p folks who have helped me along the way..

And finally

Thanks to the EFF, for their continued support of all of the world's rights in this technological era.
Thanks to all the folks running the FreeNets who continue to support the right to free access to information in this world of cynicism.
Thanks to cDc, for not selling out after all these years...
Musical inspirations: Primus, Rage Against the Machine, Jimi Hendrix, Led Zeppelin, Dead Kennedys, White Zombie, the Beastie Boys, etc, etc.

"Yes I know my enemies. They're the teachers who taught me to fight me.
 Compromise, conformity, assimilation, submission, ignorance, hypocrisy,
 brutality, the elite"
 - /Know Your Enemy/ (c) Rage Against the Machine

          - Deicide -
    deicide@west.darkside.com

DISCLAIMER

This file was provided for informational purposes only.
The author assumes no responsibilities for any individual's actions after reading this file.